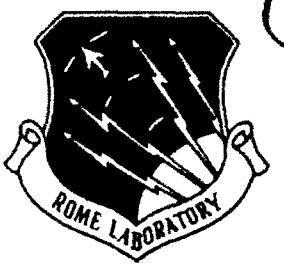
RL-TR-92-345, Vol VII (of seven)
Final Technical Report
December 1992



SYSTEM ENGINEERING CONCEPT DEMONSTRATION, Security Study

MTM Software Engineering, Inc.

Miguel A. Carrio, Jr.

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

Rome Laboratory
Air Force Materiel Command
Griffiss Air Force Base, New York

This report has been reviewed by the Rome Laboratory Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

RL-TR-92-345, Volume VII (of seven) has been reviewed and is approved for publication.

APPROVED: Frank A. LaMonica

FRANK S. LAMONICA
Project Engineer

FOR THE COMMANDER: John A. Graniero

JOHN A. GRANIERO
Chief Scientist
Command, Control & Communications Directorate

If your address has changed or if you wish to be removed from the Rome Laboratory mailing list, or if the addressee is no longer employed by your organization, please notify RL (C3CB) Griffiss AFB NY 13441. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1992	Final Feb 90 - Jul 92

4. TITLE AND SUBTITLE
SYSTEM ENGINEERING CONCEPT DEMONSTRATION,
Security Study

5. FUNDING NUMBERS
C - F30602-90-C-0021
PE - 527027
PR - 5581
TA - 18
WU - 54

6. AUTHOR(S)
Miguel A. Carrio, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
MTM Software Engineering Inc.
12110 Sunset Hills Rd, Suite 450
Reston VA 22090

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Rome Laboratory (C3CB)
525 Brooks Road
Griffiss AFB NY 13441-4505

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
RL-TR-92-345, Vol VII (of seven)

11. SUPPLEMENTARY NOTES
Rome Laboratory Project Engineer: Frank S. LaMonica/(315) 330-2054

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This final technical report documents the objectives, activities, and results of Air Force contract F30602-90-C-0021, entitled "System Engineering Concept Demonstration." The effort, which was conducted by Software Productivity Solutions, Inc., with McDonnell Douglas Corporation - Douglas Aircraft Company and MTM Engineering Inc. as subcontractors, demonstrated and documented the concept of an advanced computer-based environment which provides automation for Systems Engineering tasks and activities within the Air Force computer-based systems life cycle. The report consists of seven (7) volumes as follows: I) Effort Summary, II) Systems Engineering Needs, III) Process Model, IV) Interface Standards Studies, V) Technology Assessments, VI) Trade Studies, and VII) Security Study.

This Volume (Volume VII - Security Study), provides an assessment of security technology, an analysis of security requirements for an automated systems engineering environment, and recommendations for a secure architecture for the envisioned systems engineering automation.

14. SUBJECT TERMS	15. NUMBER OF PAGES
System Engineering, System Life Cycle Tools, System Life Cycle Environment	76
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

List of Tables

List Of Figures

I. Introduction

This work was performed under U.S. Government (Department of the Air Force), contract F30602-90-C-0021 and as authorized under subcontract No. 1991-J5012-2. The work was performed in support of the Systems Engineering Concept Demonstration (SECD) and the envisioned automated environment resulting from such, named Catalyst.

The effective implementation of a SECD security program, that insures the proper protection of classified and sensitive information, begins by addressing the subject of security early in the life cycle of the objective system. Security issues that are addressed well into the implementation phase; or those that are addressed after the fact, will result in certainty of compromise of the system information. Similarly, investigations of enabling technologies that support system implementation are not only required but should also be initiated early in the system life cycle. The investigations and technology incursions are needed to establish the feasibility and viability of the security measures needed, to provide the required degree of protection. Additionally, in any security implementation program, schedule consideration must be taken into account for the lengthy technology certification times.

II. Discussion

The Systems Engineering Concept Demonstration(SECD) effort was an exploratory development whose objective was to specify and demonstrate the concept of an advanced computer-based environment, implementable in the 5-7 year time frame, to support the Air Force systems life cycle.

The envisioned automated environment, named Catalyst, will be a set of highly adaptable and configurable "building blocks" in the form of interactive software tools and environment frameworks. When integrated with an installed computer system (hardware plus software) and other software (tools and frameworks), these building blocks will provide automated support for systems engineering.

Because Catalyst will support government and contractor personnel in the development, maintenance and enhancement of military applications, it necessarily must support applications where some or all of the information dealing with the system is classified.

With Catalyst focused on the systems engineering domain, a security compromise of trusted information can have far reaching implications that transcend the boundaries of hardware, software and firmware. Doctrinally sensitive systems, with short operational life spans, can be potentially compromised in even less time if security issues are not addressed very early in the life cycle of their corresponding support environments.

III. Objective

The objective of this effort was to provide technical analysis and support addressing automated systems engineering environment applications and security issues. The following three tasks were identified in support of the objectives:

- Security Technology Assessment
- Catalyst Security Requirements Analysis
- Security Architecture Recommendations

Task A, Security Technology Assessment, examined enabling technologies to allow practical use of Catalyst for secure applications. The technologies investigated were focused on, but not limited to, secure operating systems, trusted databases, communications, networking and host platforms. Other viable technologies were also examined for application and adaptation within the Catalyst development timeframe, i.e. next 5-7 years. Should any technology voids or deficiencies be encountered, these were also to be identified for potential research and development focus.

Task B, Catalyst Security Requirements Analysis, assessed, established and analyzed the foundation for a core set of security requirements to enable Catalyst operation in secure applications. The core set of requirements are expected to mature and be refined as they are elaborated and parsed throughout the design documentation hierarchy.

Task C, Security Architecture Recommendations, identified architectural techniques, views, constraints and approaches to subsequently assist in the refinement of a viable Catalyst architecture.

IV. Considerations

The tasks were short term in nature and not intended to be detailed assessments. It was important to obtain a sense of direction, maturity and availability on the issue of security, its promise and supporting technology.

Technology demonstrations were difficult to orchestrate due to information sensitivity on the part of developer/vendors and their certification status/schedules. Much marketing hype was found to exist on the part of hardware vendors and capabilities relative to their products. Claims exceeded expectations.

Task B, the requirements analysis task, provided the baseline set of requirements. These have been elaborated upon and subsequently upgraded into the set contained in the SECD requirements specifications for CATALYST. This task served as an initial baseline to capture security requirements and issues. As requirements matured and issues became less ambiguous, they eventually were transformed and transitioned to the specification. The SECD demonstrations provided the opportunity to refine the requirements over the span of this effort.

The sum of these tasks, demonstrations and discussions established an early infrastructure for the domain of security. Security and related issues are traditionally inadequately addressed or considered after the fact, with the exception of intelligence agencies that must deal with these issues and sensitivities on a daily basis. The subjects and views discussed in this report are intended to provide early insight into the security arena and raise issues relevant to the security domain. The information presented also provides a sound basis for the establishment of a security program for any system/software development.

Where products or vendors are identified in this document, they are cited as examples and not intended as an endorsement of the particular product or technology. Products and vendors are mentioned to establish technology credibility and implementation feasibility in support of an environment such as Catalyst. The products identified are a representative set and are not intended to convey that they are the only ones. The real test will occur when the different technologies are integrated into a CATALYST environment and scenario, and the proof of concept is verified.

V. Summary

It must be recognized that implementation of a secure SECD systems engineering environment will require the following:

- A well formulated security scenario
- An initial set of resilient and "complete" security requirements
- A mature and validated process model
- Identification of a security methodology
- Identification of a set of supporting security documentation
- A series of continuing demonstrations utilizing the environment building blocks
- A well formulated set of mission profiles and support activities
- A well formulated set of personnel roles and responsibilities
- A well integrated process model with other process models(e.g. CMM or NIST/ECMA) that can impact the overall system engineering process

An early focus and consideration to appropriate security issues and requirements is essential for the success of any systems engineering environment or program. Resulting architectures will require time consuming assessments and evaluations, hence the need to begin the security tasks early in any program's life cycle.

In the final analysis, Government security requirements for trusted levels must be adhered to. The information contained in the Table 1, identifies a range of trusted levels required to protect information while taking into consideration personnel security clearance requirements. Levels of trust at the B1 level can be satisfactorily met by the marketplace. At the B2 or above, for the CATALYST environment, the next 3-5 years appear to represent reasonable maturation times for additional product offerings. Achievement of an A1 level of trustedness, for the CATALYST environment range of functions that must be supported within the next 5 to 7 years appears questionable and introduces a higher degree of risk. A pragmatic approach to achieving these higher levels of trustedness (greater than B3) within this timeframe, would be to require supporting individuals to be cleared at the top secret level prior to joining an activity. The activity itself would require preparation for the higher clearance similar to what is done today for compartmented security.

As can be seen from Table 1, with appropriately cleared individuals at the secret or top secret level and data sensitivity at the same levels, the current state-of-the-

practice, available technology and approaches satisfy many of the CATALYST requirements and mission roles. From a security programmatic view, if properly implemented, CATALYST's feasibility can be a reality.

Table 1. Data Sensitivity and User Clearance

Maximum data sensitivity[1]

Minimum clearance or authorization of system users	U	N	C	S	TS	1C	MC
U	C1	B1	B2	B3	**	**	**
N	C1	C2	B2	B2	A1	**	**
C	C1	C2	C2	B1	B3	A1	**
S	C1	C2	C2	C2	B2	B3	A1
TS(BI)	C1	C2	C2	C2	C2	B2	B3
TS(SBI)	C1	C2	C2	C2	C2	B1	B2
1C	C1	C2	C2	C2	C2	C2[2]	B1[3]
MC	C1	C2	C2	C2	C2	C2[2]	C2[2]
	Range of Catalyst[4] Operations (shaded)						

Cells denote minimum level of trusted computer system criteria

LEGEND

U = Uncleared or Unclassified
N = Not cleared but authorized access to sensitive unclassified information or Not classified but sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Backgound Investigation)
TS(SBI) = Top Secret (Background Information
1C = One Category
MC = Multiple Category

1 Environments for which either C1 or C2 is given operate in System-High security mode. No minimum level of truse is prescribed for systems that operate in Dedicated security mode. Categories are ignored in the matrix, except for their inclusion at theTS level.

2 It is assumed that all users are authorized access to all categories present in the system. If some users are not authorized for all categories, then a class B1 system or higher is required.

3 Where there are more than two categories, at least a class B2 system is required.

4 Base range of Catalyst operations is shown. Higher levels of operation may be achieved with to-be-specified enhancements.

** Indicates that computer protection for environments beyond that risk index are considered beyond the state of current technology. Such environments must augment technical protection with personnel or administrative security safeguards.

Source: DoD Computer Security Center, *Technical Rationale Behind CSC-STD-003-85:Computer Security Requirements – Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, CSC-STD-004-85, 25 June 1985.

VI. Security Synopses

A. Task 1 - Security Technology Assessments

A.1 Introduction

The changing nature of terrorism and espionage, in light of world events, has embraced new approaches with respect to the traditional concept of return-on-investment(ROI). The ROI of stealing something for a fraction of the cost that was required to develop it has come into the modern world of computers, their security and environments. The cost of penetrating or disrupting a computer network compared to the loss incurred from its disruption provides an excellent ROI to the terrorist. Terrorist activities have taken on added significance when applied to the increasing dependence of the U.S., and DOD in particular, on computer technology.

Winn Schwartau, a computer security expert, in writing his recent novel "Terminal Compromise", hopes that his latest book will "shake us out of our complacency on security". Similarly, Walter R. Houser, software specialist/writer for Government Computer News, in his September 30, 1991 article, is concerned that the "frightening activities", described in Schwartau's book, "are well within the state-of-the-art of computer espionage". According to Schwartau, several Government security agencies have confirmed to him that the threats posed by a coordinated group are enormous. The increasing concern is that with recent military actions undertaken in the middle east(i.e. Desert Storm), future terrorists will now covertly direct their activities at such enterprises as telecommunications, banking, health, credit, airline and Government computer networks as a more cost effective means of accomplishing their political objectives. This terrorist potential, together with the seeds of "inspired and challenged" computer hackers and disgruntled employees pose a significant threat to any computer network, especially DOD's.

The security threat posed to computer networks is also shared by the Pentagon's Corporate Information Management chief, Director of Defense Information, Paul Strassman. He expressed serious concern on the protection of DOD information and the Government's ability to prevent disasters unless an initiative is undertaken. Mr. Strassman at the Government Computer News Forum, held at the National Press Club, Washington, D.C.,(9/91), said, "Local area network security lapses have left open the gate to serious disaster for the Defense Department". Furthermore, at this forum to industry and Government, he reiterated that: "There is no such thing as information that is not classified. A particular record may not be classified in isolation. But the cumulative reading of

a stream of messages about spare parts from one of our depots where we keep certain parts gives a tremendous amount of information to anybody who wants to listen. I'm not satisfied as to the protection of that traffic".

Mr. Strassman has indicated that the issue of security was very important to the CIM initiative. There is a "gold nugget" reserved for any breakthroughs in this area. Gold nuggets are those areas of high interest and bearing relative to CIM implementation solutions and associated barriers that must be overcome for CIM to succeed.

Security issues and the protection of information have taken on added significance at the National Institute of Standards and Technology(NIST)[GCN91]. NIST is one of two major Government agencies with responsibility over this area(NSA is the other agency). A recent initiative was launched by F. Lynn McNulty, Associate Director for Computer Security at NIST's Computer Systems Laboratory(CSL). NIST is undergoing a movement with the Office of Personnel Management (OPM) to formally recognize a "Computer Security" job classification at CSL. "The objective is to show the importance of the area(security) and that it should not be considered as a part-time duty. Professionalizing the whole field would force agencies to recognize it as a separate and distinct career".

A.2 Discussion

The complexity and interrelationships of design, hardware and software elements necessitate that a holistic systems view(i.e. a systems engineering view) be adopted in order to reduce the threat to computer systems and their environment. Prior industry and Government initiatives have primarily focused on homogeneous and isolated views of such(i.e. either all software or all hardware or documentation). Examples of some of these are: CAIS, STARS, PCIS, NASA SSE, SLCSE, NASEE, CALS, ALS and EIS. The protection of information and systems resources can only be effectively managed if the respective views of hardware and software are considered in a unified and consistent manner.

Conspicuous by their absence(of the cited examples) have been systems engineering environments. The recent advent of the Air Force's CATALYST environment represents one of the few DOD heterogeneous views, (i.e. systems engineering), known to date. The full value of such has not been recognized, and whose potential is underestimated. Systems engineering environments (SYSEE's) provide a unified solution and effective coupling between the domains of software and hardware engineering. SYSEEs provide the proper level of abstraction in which to resolve system issues affecting both software engineering environments (SEE's) and hardware or computer-aided design (CAD) environments. From a security point of view, however, the synergism and

leverage to be gained from SYSEE's must be tempered by a rigorous discipline of management and operation. SYSEE's extensibility and flexibility across the life cycle present the potential to compromise even greater amounts of information than ever before. The compromise will occur unless security and configuration management are made an integral component of them. Just as in development the antithesis of architectural openness is formal design and methodology rigor; user accessibility and flexibility are the antithesis of information integrity and security. Thus, a careful balance between these elements must be maintained and applied early enough in CATALYST's life cycle for an implementation methodology to be effective.

Essential to the success and security capability of CATALYST are three enabling technology areas, that when applied together, can provide effective protection from unauthorized individuals and those attempting to gain access to the information cells contained within the environment. No one technology should be depended on solely. But their coexistence within a deployed environment, together with other measures, can provide a high integrity trusted security envelop.

The enabling technologies fall into the following three categories:

- Operating System
- Data Base
- Network

Rather than focus on potential and as yet untested products; maturing and state-of-the-art available products will be discussed in each technology area. The existence of these products can provide a degree of confidence that the security measures and technology required by CATALYST in the next 2-4 years, are available and can be used to establish proof-of-concept. It can then be reasonably expected that this lead time is sufficient for other emerging technologies in these categories, along with those scheduled to be tested by National Computer Security Center to provide a greater diversity and choice beyond this timeframe.

A.2.1 Operating System Technology

Much effort has been expended over the last decade in secure operating system (SOS) technology by both industry and Government. Several companies have been developing products and conducting research in this area(TRW, Honeywell, DEC, Informix, Verdix, Oracle, Harris and Addamax) to name a few. DOD's National Computer Security Center(NCSC) has published the Rainbow Series of documents(by virtue of the color of their covers)[NCS88a,b,c,d], on security, certifications and related topics. Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, (known as the orange book

[NCS87]), on trusted operating systems, is probably the best known in the series. The technical community is aware, for the most part, of the seven levels of compartmented trust and requirements for the processing of classified information(the reader is directed at the standard for more information). The levels are identified in Figure 1. A lengthy and rigorous process exists for certification requiring several years before a developer or vendor can acquire an NSCS certified rating. Of the seven levels identified, industry can reasonably deliver main frame and workstation products in the C1 through B1 categories. For the most part, products at or higher than the B2 level (i.e. B3 through A1) are emerging with most currently undergoing evaluation or still several years from certification. Addamax and Oracle are estimated at being 12 to 24 months from certification at the B1/B2 level.

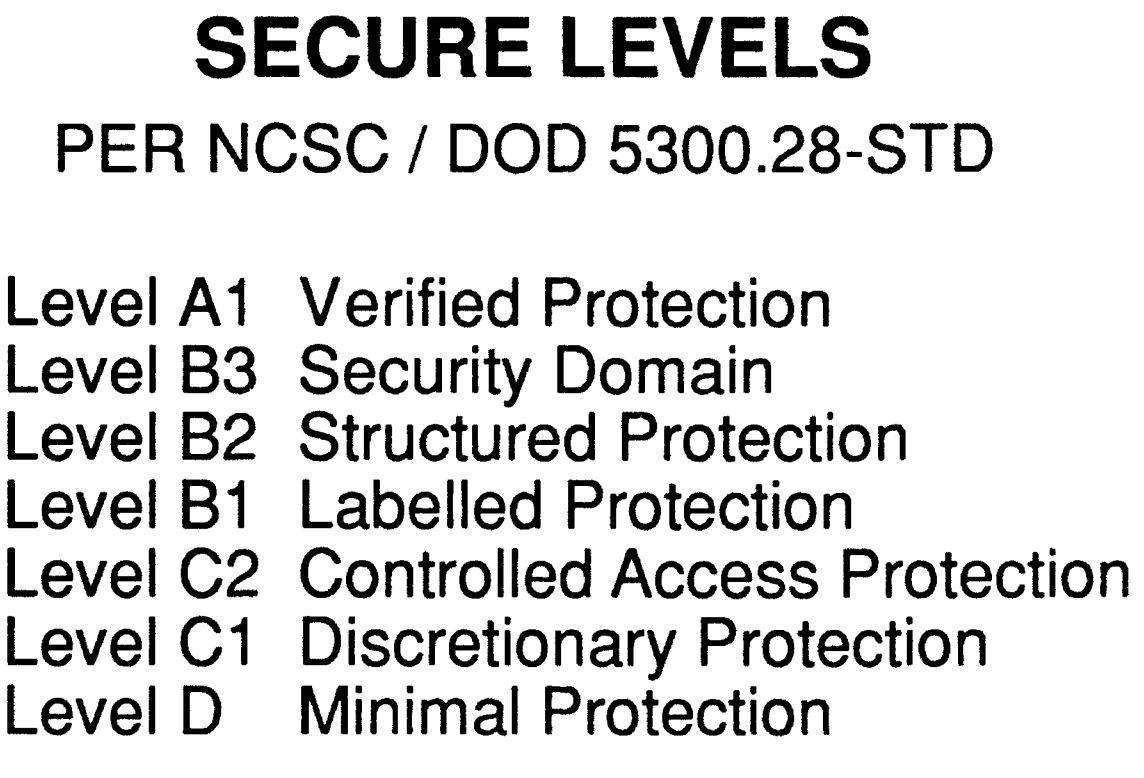


Figure 1. Secure Levels

Additionally, much work continues on SOS such as the UNISYS initiative, under the STARS Program and the JIAWG (Air Force)[JIA91a,b]. Secure operating systems represent the nucleus of the security protection domain. Much has been

written on them, they remain in the forefront of discussions, and will not be discussed at great length in this paper. Other security technologies/issues will be discussed henceforth.

A recent and emerging area, driven by the widespread use of the workstation is the compartmented mode workstation[WOO87] to support the increasing security needs of users on this type of hardware. The demand for engineering workstation capability, the extensive third party software products available on them(CASE, CAD, CAM,et al), and their decreasing prices establish them as a viable market entity. The increasing performance envelop of personal computers, and the decreasing price of the engineering workstation has also established an encroaching grey area where these two product families, once viewed as separate, now overlap and compete with each other.

Five companies currently have on-going programs with the Department of Defense to develop a compartmented mode workstation (CMW):

- ADDAMAX - Zenith 386, System V, OPENLOOK
- DEC - VAXSTATION, ULTRIX, MOTIF
- IBM - RS 6000, AIX, MOTIF
- Secureware - MacIntosh IIX, A/UX, MOTIF
- Sun Microsystems - SPARC, SUNOS, OPENLOOK

CMW's are platforms that have a trusted operating system with a trusted window management system. The workstation can support compartmented mode operations and provide for separation of sensitive compartmented information (SCI).

One particular effort, Addamax's, will be discussed by virtue of the proliferation of PCs and their increasing performance and competitiveness with the workstation market. Their hardware platform is the INTEL 80386/486, UNIX based, with the OPENLOOK graphical user interface. This effort is jointly sponsored by ADDAMAX and Harris Corporation and is designed to meet the class B1 trusted criteria of DOD 5200.28 STD. The software is releasable on 3.5" or 5.25" floppy disks and 1/4" cartridge tape. Mandatory and discretionary access control capabilities are supported with auditing, identification and authentication. Secure bootstrapping and trusted window applications are also provided, along with operation in a trusted TCP/IP environment.

All audit information is kept in a separate audit log file that can be accessed by an information system security officer. Auditing criteria can be further selected and grouped to isolate patterns of attack or degradation for subsequent analysis.

A complete set of user and administrator documents is available, that includes:

- Security Features User Guide
- Trusted Facility Manual
- Security Reference Manual
- User's Reference Manual
- System Administrator's Reference Manual
- Programmer's Reference Manual

The Addamax software is portable to any 386/486 machine in the marketplace. Thus, security to the PC side of the environment is provided. Addamax is approximately seven(7) months into its security evaluation and is in a beta mode. A TEMPEST version option is offered, and future plans with CMC/Rockwell International are under way to supply an intelligent ethernet board which implements the DNSIX trusted TCP/IP networking protocol per the Mitre/DIA specification.

The Beaver Computer Corporation[CEN91] is also developing the first secure Intel 386/486 notebook computer. It uses a special security co-processor based on NIST's DES encryption algorithm. This effort is being performed in conjunction with SAI Technology Inc.

Summary

The lengthy Government certification process and limited product availability reveals that it will be 3-5 years before additional approved products are in the marketplace. Similarly, Government standardization efforts (e.g. public key encryption standards) from such groups as NSA and NIST are still several years away. The current standards philosophy appears to be to await a greater diversity and availability of products, and see if a defacto industry standard emerges[FCW91a]. There is some current controversy on the public encryption standard between industry and the Government[FCW91b]. Thus, any longer term solutions (greater than 4 years) will be influenced by the new and emerging products and approaches that continue to mature over the near term. The next 2-3 years represent an impacting timeframe for any environment that will require security measures and protection, such as CATALYST. Any long term security measures will therefore require careful orchestration and monitoring of on-going activities, together with periodic proof of concept demonstrations. This will ensure that viable implementation solutions can be identified to enable technology insertion and transition.

The most critical component of the three technology areas is clearly the secure operating system. It is also the most complex and difficult to certify. Much has been written on SOS's and few have been certified. While DOD would be the beneficiary of numerous SOS programs and products, it is clearly not as influential in the commercial marketplace, nor is DOD's influence over the latter expected to increase in the foreseeable future. Additionally, DOD's transition to the Ada language is expected to create "platform stress", until a greater use of Ada is encountered in the commercial arena. DOD's focus on the Ada language, and industry's on the C language, is contributing to the apparent schism of product focus and availability. However, an increasing awareness of the need for secure and trusted products in industry and the Government is clearly understood by all.

A.2.2 Database

Protection of information contained within a database, particularly one accessed by individuals with different levels of security, becomes the second most important technology area. Many issues arise in the database arena, several of which are considered essential for the protection of information:

- Access to the database
- Compartmentalization
- Polyinstantiation
- Operating system interface

Access - Access controls must be available to the database manager or responsible administrator to provide information access to only appropriately cleared individuals, and with an identified need to know domain.

Compartmentalization - The need to compartmentalize the database becomes critical in a system where classified, as well as unclassified information coexist. Additionally, within the classified compartment, different levels of information security are contained(i.e. Top Secret, Secret, Confidential) [FIT91]. Information must also be protected from covert channel access [BAD91] (i.e. alternate or back door channels that can bypass database mechanisms to obtain information).

Polyinstantiation - Polyinstantiation [SAN91] refers to multiple instances of data (e.g. two or more rows in a database that have the same apparent primary value). Without compromising the sensitivity of records or data, schema must be available to identify information declared with the same label/name but belonging to different individuals with different levels of security access. To maintain information integrity, individuals with access cannot be made aware of the existence of higher classified information with the same record declarations.

Operating System - The interface and level of dependency on the operating system can impact the degree of security available within an environment. System performance can also be affected by the degree of handshaking and dependencies required between the OS and DB. Covert channel protection [BAD91] also becomes an issue if the DB can circumvent OS or network security measures, and vice-versa.

Oracle Corporation has two maturing products that are undergoing evaluation at the NCSC and will be available as alpha releases in 1992. These products are currently available for utilization in proof-of-concept experiments and projects. Since their trusted products are also intended to be upwards compatible with current Oracle offerings in the marketplace, availability of these trusted versions enables early familiarization within their customer base. Oracle has two offerings in the database area worthy of note, since they are well into their evaluation period(8 months) with NSA, and expect to release Version 7 early in 1992. Release of Oracle products will not be contingent on NSA certification. Oracle was selected as a focus in this report for the following reasons:

- NCSC Product Submission: Oracle has submitted two products, Oracle Version 7 and Trusted Oracle, for NCSC evaluation. Oracle V7 is aimed at the C1 level of classification, while Trusted Oracle is aimed at the B1 level. The products were submitted in April 1991 to the NCSC. Oracle will release the products in 1992 as alpha releases while NSA evaluations are on-going.
- DOD Projects: Oracle is currently involved in several Government projects. Two of which are NSA's multi-level security (MLS) experiment and the other is the Air Force's Seaview. The NSA project involves a "Red October" scenario whereby information is being presented at consoles to operators from different sources with different classifications in the course of pursuing a submarine. Seaview is the Secure Distributed Data Views[RAD89] secure system research project, lead by SRI International, and sponsored by Rome Laboratory. Part of Seaview supports the building of a class A1 system ported to GEMINI Computer's target hardware and the GEMSOS operating system platform.
- Availability: Oracle products are currently available on two platforms, DEC under VMS, and HP under UNIX. Future targets identified are Data General's AViiON UX and IBM's RS 6000, AIX.

- The products support both mandatory and discretionary access control measures; and support many of the compartmentalization and access control features required per the NCSC 5200.28 STD. The features are too numerous to list and product literature should be consulted. A few relevant ones will be mentioned however:
  - Multiversioning is provided to assist in the management of polyinstantiation
  - The products can function with either a secure operating system or an unclassified one
  - Current product upwards compatibility is provided, thereby facilitating database upgrading and transitioning of technology
  - Two operating modes are possible for use with a secure OS(OS MAC) or an unsecured one (DBMS MAC). In the OS MAC mode Trusted Oracle minimizes redundancies between the OS and RDBMS(user identification and authentication is defined at the OS level and is not duplicated with the DB transactions). Other similar relationships are established to provide efficiency and performance.
  - The Oracle products can function in a distributed environment. Trusted Oracle does not modify or inhibit connectivity features and functions of an OS and/or network.

Summary

Database technology is rapidly maturing with a sufficient availability and diversity of products in the marketplace. The next generation of database technology products is departing from the relational views to that of object views-Database Object Management Systems/products. The companies identified are currently developing or have developed object oriented products(Oracle for example already incorporates several object views within their database technology in their new releases). However, object view technology is still in its embryonic stages with few mature products available.

Other companies are developing secure database products that over the next several years are expected to provide market diversity. Some of these are:

- Atlantic Research Corp. — Multi Level Secure Database Protection Mechanisms
- DEC — Relational Database(RDB), B1
- Informix Software, Inc. — Secure RDBMS, B1,C2
- Sybase, Inc. — Level B2 database product
- Teradata Corp. — DB Machine(DB1012), B1,C2

In summary, database products provide trustedness up to the B1 level. Products at the B2 level and above remain questionable and must complete their certification in the database arena.

A.2.3 Networks

Secure Network Protocols - Of the three technology areas identified, networks is the newest one relative to security. The significant increase in networks and networking over the last decade has focused attention in this area. While secure network protocols using TCP/IP[FUT91] are available, they are considered as another link in the security chain. Secure network protocols(SNP) provide added security measures to classified information and prevent it from being inadvertently interleaved and compromised at network locations other than the appropriate one. However, trusted network protocols are ineffective as a primary security measure once an individual has penetrated or accessed the network.

One of the two weakest security links in a network of computer hosts, servers and target systems is the network protocol scheme used. The other is the trusted X window schema, discussed in the CATALYST Security Architecture Task Summary, section VI, C. The TCP/IP protocol developed for ARPANET represents the most popular one used within the Department of Defense. Recent work done at AT&T [FLI89][FUT91] in conjunction with the Wollongong Group has produced a security enhanced TCP/IP called MLS/TCP[1]. The latter is fully compatible with existing TCP/IP implementations and addresses the critical problem of labelling. All data in a multi-level secure system must be labelled, per the Trusted Network Interpretation [NCS87], to enable the host to make access control decisions. Provisions for labelling enables a strong linking between the data and its label to establish mapping relationships between multiple formats

---

1 TCP/IP - Transmission Control Protocol/Internet Protocol. MLS/TCP - Multi-level Secure/TCP.

and their representations. MLS/TCP is currently compatible with System V/MLS, the multi-level secure enhancement to AT&T's System V UNIX[2], operating system. System V/MLS[3] is certified for B1 operation by the National Computer Security Center.

Military Standard 1777 specifies the internet protocols security options and other related security changes under review, such as the Basic Security Option(BSO) and the Extended Security Option(ESO). Some of the IP security options include identification of security level, compartments, handling restrictions and transmission control code. While BSO and ESO are administered by DOD, there are other commercial security options supported by vendors developing secure operating systems. An exa nple is the Commercial IP Security Option(CIPSO) permitting security related information to be passed between systems in the commercial or open system environments. MLS/TCP permits operation in both DOD and commercial network applications since compatibility options have been provided for both BSO/ESO(DOD) and CIPSO modes. Additionally, the protocols can be concomitantly employed in both untrusted and multi-level security network applications that are characterized by a client/ server architecture, where a defined application layer protocol is implemented. The protocol can be utilized in configurations where there are trusted as well as untrusted servers. In this manner, a trusted server can gain access to other system resources and specific network connections with a specific session label and preclude or bypass the untrusted link.

The particular MLS/TCP implementation is also compatible with other trusted networks such as Verdix's VSLAN network rated at B2 by the NCSC. VSLAN labels can be accepted and converted to either CIPSO or BSO labels for subsequent passing to the internet protocol layer, i.e. network layer of the Open System Interconnection (OSI) Reference Model. Other benefits accrued by use of MLS/TCP is that a simple ethernet network can be a trusted network if all of the hosts in the network are trusted. For this network, the security parameters are passed in the MLS/TCP protocol and a separate security interface is not required.

---

2 UNIX is a registered trademark of AT&T, UNIX Systems Laboratories.

3 Defined in "System V/MLS 1.1.1 Trusted Facility Manual", AT&T, 13 June 1989.

Thus, the labelling options provided in MLS/TCP enable the passing of data to/from trusted and untrusted hosts within a network to establish a communications link while protecting the information. The implementations are designed to satisfy the Mandatory Access Control and Audit requirements of [NCS87].

TCP/IP can be connected to many types of networks such as ethernet, token ring, or a serial RS 232 line. Secure TCP/IP can protect the data only while it is in the host system. External to the host, security responsibility is dependent on the network capability. The latter is usually handed off to an encryption device (cryptographic unit) or an end instrument.

Another significant issue to be addressed in networks is the access control to the network at user entry points. The most common means of controlling end points is by the use of an encryption device, e.g. cryptographic unit. More recent cost effective developments, e.g. STU III, provide voice and removable encryption modules that can be placed at users location. These devices can be located on desks, and once the encryption module is removed, the unit can be left unattended. Employment of DOD encryption devices at these numerous entry points is the most effective solution, but can be a very costly and a logistically burdensome activity. Additionally, distribution and updating of encryption keys can be a complex security and labor intensive task. The large number of users encountered in a network burdens management's capacity as well, to oversee the network.

Secure Access Control - New technological breakthroughs and cost-effective approaches such as those developed by Security Dynamics, provide viable alternative approaches to controlling network access. Furthermore, network management is simplified and users are not required to invoke sensitive logon procedures. The Security Dynamics approach also provides a solution to mobile subscribers in a network requiring access from different entry points. This unique approach, exploiting 80186 and liquid crystal technology, provides user access control at any entry point into the network.

The concept is based on a traditional approach to protect access to a network and analogous to employing encryption units at network entry points. Except that instead of using encryption devices, a security card containing the keying algorithm(SecureID card) is used as the entry point protection device. The device is compact, measuring 2 1/4 inches by 3 1/4 inches and approximately 1/16 inch thick and can be used with other security devices(e.g. picture ID and physical entry(key) devices. The following product overview is extracted from the NCSC Final Evaluation Report on: Access Control Encryption System, CSC-EPL-87/001, Library No. S228,455 on Security Dynamics Products.

Product Overview- The Access Control Encryption (ACE) system is an integrated hardware/software package which provides user identification and authentication and authenticated connection mechanisms for a host system. In addition, it audits all ACE mediated access attempts to the host. The ACE system is composed of two components, the Access Control Module (ACM) and the SecurID card. Figure 2 shows the components and the Security Dynamics concept. The ACM can also be configured such that it authenticates itself to the user before asking the user to give authentication data, thereby providing an authenticated connection. The SecurID card generates a series of pseudo random numbers(PRN). One such PRN is always displayed in a liquid crystal display on the face of the SecurID card, and is used by the user, in addition to a personal identification number(PIN), to identify himself to the ACM.

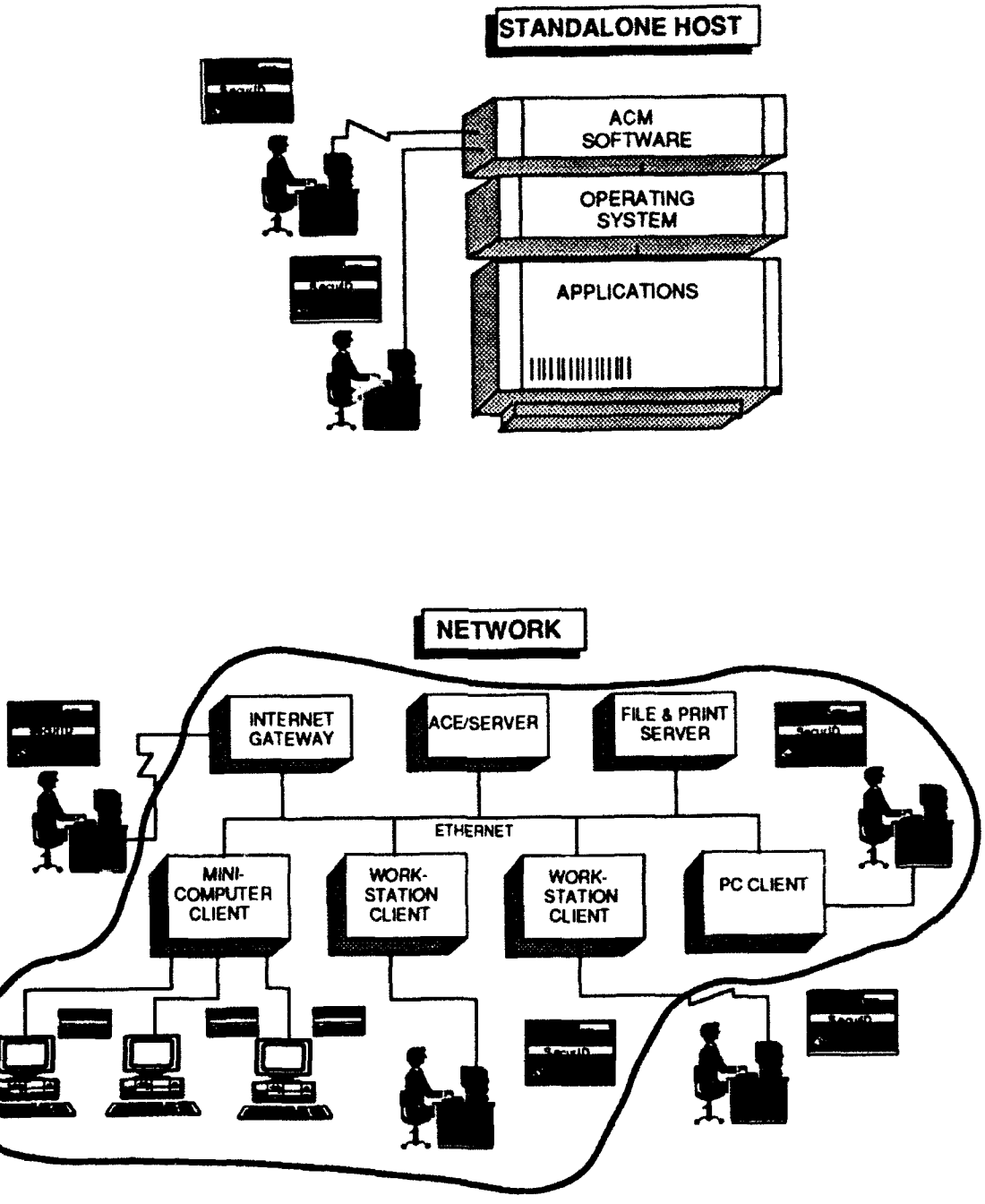


Figure 2. Secure ID Card Authentication

Identification and Authentication- Before gaining a connection to the host computer, each user must enter a valid PIN and PRN. These values serve to identify and authenticate the user to the ACM, and implicitly authenticate the user to the host machine. The PIN/PRN combination can be entered one of two ways, determined by the initial system configuration. The first method is to enter the PIN followed immediately by the PRN. The other method involves adding the PIN to the PRN without carry. This method effectively hides the PIN, because the constant PIN is being added to a seemingly arbitrary number creating what appears to be an equally arbitrary number.

Each SecurID card has a serial number and at least one PIN which are unique to any given ACE system. It can be changed only by the ACE administrator, who executes an appropriate function to generate a new PIN. The PINs can only be randomly generated by the ACM, and cannot be set manually. To obtain the newly generated PIN, the card holder must enter the card's serial number and current PRN at a standard passcode prompt, after which the mew PIN will be displayed on the terminal for approximately ten seconds. PIN data cannot be retrieved from the ACM, even by an ACE administrator.

The PRNs generated by the SecurID cards are seemingly random. The card's PRN generating algorithm is synchronized with a similar algorithm in the ACM. At predetermined intervals of time, determined by the purchased configuration, the PRN changes. Any variations in the two clocks involved are handled by a proprietary method which seems to work very well.

At ACE system generation time, each card can be programmed to self-destruct after a predetermined period of time. Destruction consists of the card erasing all of its memory, rendering itself useless. It can then never be reinitialized or reused for its original purpose. The administrator can also enable and disable individual cards for access, at the ACM.

Access to the ACM while under duress can be detected by the ACE system. This is accomplished through the use of a duress PIN. This alternate PIN seems to function exactly as the standard PIN would, except the system realizes that the user is under duress and can send out the appropriate alarms.

The system can also detect some forms of unauthorized access attempts. Repeated attempts, the count of which is ACE administrator settable, to enter an invalid PIN and a valid PRN result in the card associated with the given PRN being locked out of the system. The presumption being that the card has been lost or stolen and is in unauthorized possession. Repeated attempts to enter a valid PIN and an invalid PRN results in, after a valid PIN and PRN are entered, the user being asked for the next PRN. This is to insure that an unauthorized individual has not successfully guessed a correct PRN once.

The ACE system provides comprehensive audit capabilities for all accesses to the ACM. The audit records can be viewed only by an ACE system administrator. The audit information is stored in Random Access Memory in the ACM and is protected by battery backup.

The Security Dynamics products are also available and can be integraied for use with the following products:

- DEC VAX/VMS
- IBM MVS & RS 6000
- Sun SUNOS
- Silicon Graphics
- Tandem

PC's can be connected via any 300 to 9600 baud (limited 19.2kb), full or half-duplex line; using RS-232/RS-422A/ asynchronous, ASCII interface. While the NSA tested version was an 8 to 128 channel capacity version, current versions have 256 ports and can accommodate up to 12,800 users.

An examination and evaluation of the passwords used in their approach has been performed by MTM Engineering, in accordance with DOD Password Management Guideline, CSC-STD-002-85. The 6 to 8 digit password length, with the accompanying 4 digit PIN easily satisfies a maximum lifetime of 12 months on a 1200 baud rate line, and a probability of guessing a password of 1 in 1,000,000.

The Security Dynamics approach represents an available and cost effective per line solution for under a $100.00 per line, plus the cost of the ACM module. The latter can vary from $4K to $32K(CRAY System version), per concentrator(multiplexer). The product is well documented with a User's Guide, System Administrator's Guide and software manual.

Summary

The three products reviewed (ADDAMAX, Oracle and Security Dynamics) represent solutions that can be implemented in the near term, and provide a longer term solution as well. Certainly this is sufficient time to enable other products in testing or about to enter testing to be certified and provide CATALYST diversity and extensibility.

A more indepth assessment and evaluation of these and other products identified is recommended to refine the security "blanket" required by CATALYST. A number of other documents and product literature have not been received from vendors and developers(e.g. forthcoming CMW product literature from Hewlett Packard). Should these documents become available prior to the

final report, some of this information will be incorporated into the updated document.

It is recommended that a CATALYST security prototype scenario be developed to demonstrate proof of concept. The prototype scenario should include at least one enabling technology product in each technology area, using both PC's and workstations.

It is recommended that a more in-depth evaluation of the emerging trusted X window applications [EPS91] be made to insure support to the CATALYST needs and views. The extensibility of CATALYST views may necessitate additional security refinements beyond those currently identified. Similarly, cross fertilization with projects such as Seaview is recommended. It is recognized that as CATALYST system requirements mature, subsequent and concomitant refinements will also be required to security requirements respectively.

B. Task 2 - Requirements Analysis

B.1 Introduction

This review of the System Specification for the Catalyst System, document SSS-90-001, dated 3 August 1991 is in support of the Requirements Analysis Task[ROM91]. It is the objective of this review to assess and update, where appropriate,the sufficiency of requirements contained in the system specification, and to allow use of Catalyst for secure applications. The conclusions are based on the following:

- Review of the SSS-90-001 System Specification
- Review of the SS/DD-91-001 System/Segment Design Document for the Catalyst System.
- Security Technology Assessment Study performed under Task 1 of this subcontract.

B.2 Discussion

Security requirements are contained in SSS section 3.3.2 titled "System Security"[ROM91]. A requirement numbering system is used in this document consistent with SECD paragraph numbering, whereby the system security requirement number is identified as **SYSREQ 514.**

SYSREQ 514 is further decomposed into three sub-categories:

- Sub-category 1- Secure Operational Modes, SYSREQ 514.1
- Sub-category 2- Discretionary Protection Support, SYSREQ 514.2
- Sub-category 3- Mandatory Protection Support, SYSREQ 514.3

Sub-category 1 discusses classified operational modes that CATALYST is to support and as identified in the National Computer Security Center, Glossary of Computer Security Items, NCSC-TG-004, Version 1. Two modes are discussed- Dedicated and System High. A dedicated mode requires users to be cleared with a need to know for all of the information contained within a system. Whereas in a system high mode the user has a need to know for some of the information contained within the system.

Sub-category 2 discusses queries of the operating system, the definition and enforcement of information access privileges, access restrictions and audit mechanisms.

Sub-category 3 discusses security level identifications, tagging of objects, and automatic notification of security problems.

The CATALYST mode and state representations of Figures 3 and 4, reveal that several views of security issues coexist and must be addressed to establish a viable set of security requirements and an implementable program. In order to maintain the integrity of such an environment and effectively protect the information contained within each of these individual views, reference to Figure 5 is made. Every individual piece of information(i.e. objects, design representations, models, prototypes, reusable library components, and documentation) is considered from two basic perspectives- an external threat and an internal threat. The external threat is that which arises from the classical enemy agent or individual attempting to gain access to the network or information contained therein. For the most part, physical security is a major deterrent in this case. The more complex threat comes from the electronic attempt to gain access via some network or terminal entry point for the purpose of disrupting the environment, gaining valuable information or introducing a foreign agent (e.g. virus).

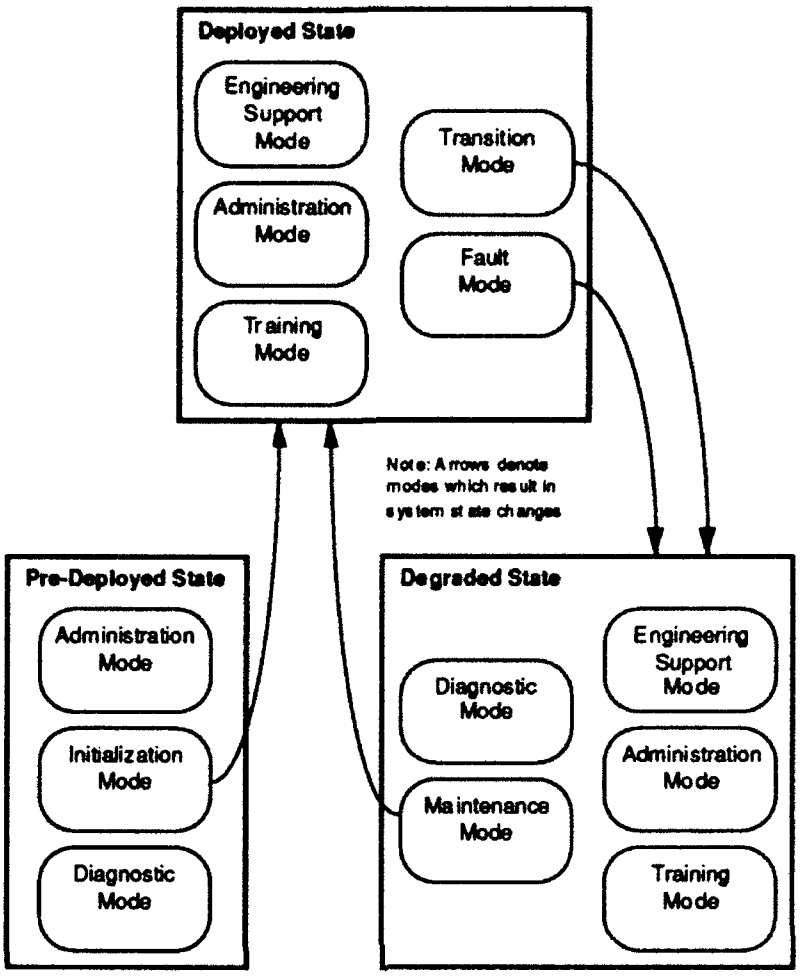


Figure 3. CATALYST States and Modes

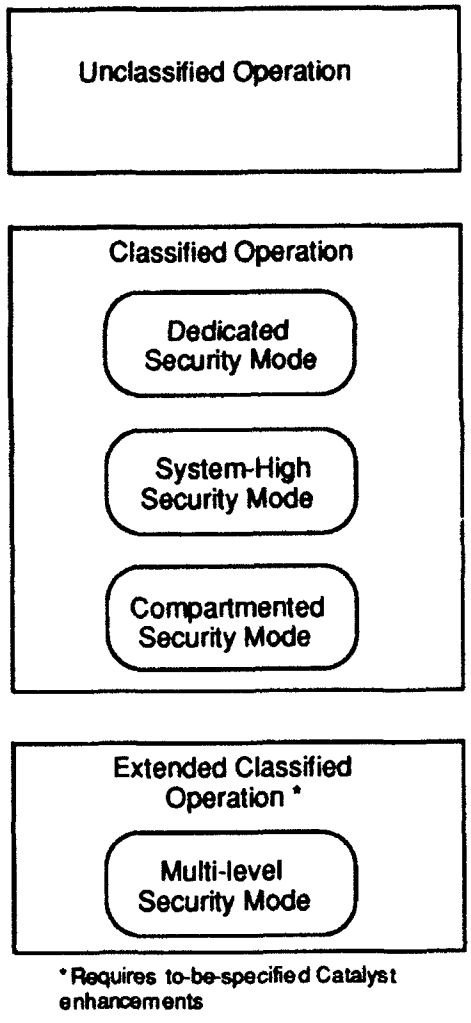
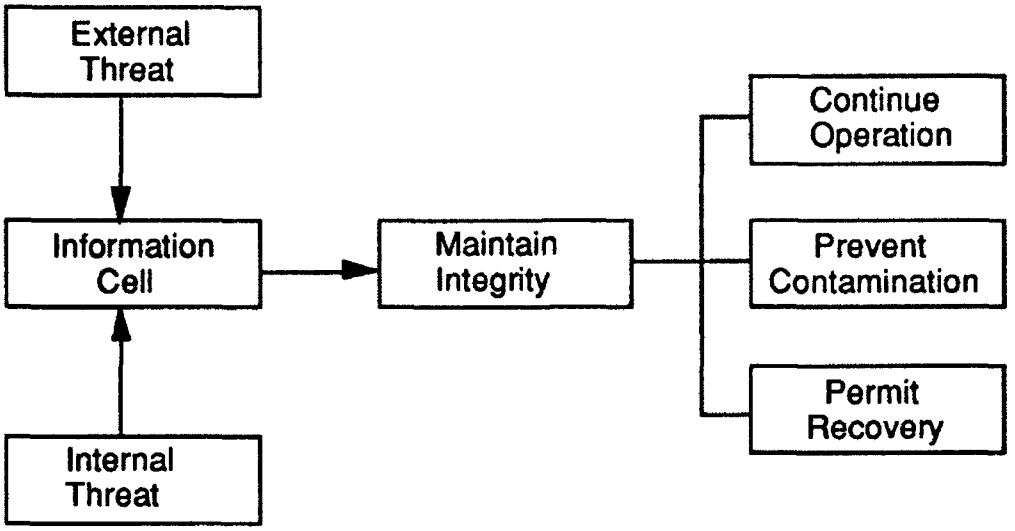


Figure 4. CATALYST Modes and Operations



TO PREVENT CONTAMINATION: From something or someone whether intentional or unintentional

TYPES OF INFORMATION:

- DESIGN
- DATA (PERFORMANCE, TEST, CONFIGURATION)
- MANAGEMENT (COST, SCHEDULE, STATUS, CONFIGURATION, DEPLOYMENT, PERSONNEL
- THRESHOLD/BOUNDARY VALUE/CONSTRAINTS
- TEST (SENSITIVITY, PARAMETRIC)
- PDSS (SENSITIVITY, TURNAROUND, FIELD SUPPORT

INTEGRITY: MUST MAINTAIN THE SUPPORT FUNCTIONS OR OPERATION WITH CONCOMITANT DAMAGE ASSESSMENT CAPABILITY

Figure 5. External + Internal Security Threats

The internal threat arises from individuals working from within an organization using CATALYST and attempting to gain access to information cells or the more extensive environment(i.e. an implementation scenario where CATALYST would be supporting a number of target systems such as in post deployment support). Similarly, the internal access to information cells is desired to:

- Obtain the information for its value
- To disrupt the environment
- To introduce foreign agents

Internal threat security must also guard against disgruntled employees that will attempt to "get even" via disruption to CATALYST.

The importance of security and the protection of CATALYST information cannot be underscored. Furthermore, security is now viewed as a key element in light of the diversified modes and applications that CATALYST is to be employed across. To adequately and more appropriately address the issues of security, the view of Figures 3 and 4 are identified. The states and modes contained in this representation enable several different views of requirements to be grouped in a more uniform and representative manner. The security views contained in the figure are supported by the suggested specification outline of Figure 6. The following comments and rationale are presented to support the views of Figure 3 and 4 relative to security:

- **Multi Functional Capability**: Common CATALYST software and hardware is utilized to support different states(a deployed state and a pre-deployed state). While these two states differ in function and sensitivity(e.g. critical mission support operation versus personnel training support operations), a less sensitive mode(training) may be deactivated and required to rapidly transition into a mission support mode. Thus, security issues and concerns, if they are not addressed appropriately and apriori, may result in the inability, tardiness or ineffectiveness of a training mode system or component thereof to be transitioned to support a critical mission support operation.
- **Architectural Flexibility:** The architectural view of the figure does not compromise design or developer domains to make design decisions since it is still at a high enough level of abstraction.
- **Transition Flexibility:** The representation allows one to transition from normal or operational modes to degraded ones or vice versa. This view provides the ability to assess the degree of potential contamination(if any) to security in going from a stable state of operation to an unstable or degraded one.
- **Domain Breadth:** The representation also reveals the breadth and scope of the security problem as more than just a discretionary or mandatory one.
- **Configuration Management:** The views depicted establish the essential need for configuration management foundations(despite the fact that it is mandated per NCSC requirements at security levels of B1 or above[NCS88c], and strongly recommended below this level).

- **Role Identification:** The views shown facilitate the identification of personnel responsibilities and function roles. This allows the identification and assignment of mission profiles and specialties for individuals supporting CATALYST.

Suggested New Outline

System Security Requirements (Sys_Req 514)

1.0 Secure/Compartmented/Operational Prime Modes:

1.1 - Secure Operational Mode
1.2 - Engineering Support Mode
    1.2.1 - Classified
    1.2.2 - Trusted Computer Base Operation
1.3 - Administrative Support Mode
    1.3.1 - Classified
    1.3.2 - Trusted Computer Base Operation
1.4 - Training Support Mode
    1.4.1 - Classified
    1.4.2 - Trusted Computer Base Operation
    1.4.3 - Sensitiv Initialization

2.0 Protection Support:
2.1 - Discretionary
2.2 - Mandatory
2.3 - Submode
    2.3.1 - Single User
    2.3.2 - Multi-user
    2.3.3 - Network
    2.3.4 - Transition
    2.3.5 - Fault/Diagnostic/Maintenance
2.4 - Recovery

3.0 Configuration Management:
3.1- Secure Configuration Management
3.2 - Certifications

4.0 Administration/Responsibilities:
4.1 - SecurityAdministration/Responsibilities
4.2 - System Administration/Responsibilities
4.3 - Personnel Responsibilities

Appendix A - Requirements Considerations

Figure 6. Suggested Specification Outline

The CATALYST environment shall support activities across different information domains (ID's) that vary in scope and magnitude. The information domains can be comprised of the following:

- Information domains that consist of broad applications areas (AA), i.e. functional areas that cover the military theater, battlefield or operations scenario.
- Information domains that consist of the applications systems (AS), such as Mission Critical Computer Systems (MCCS), AS host support systems and target support systems
- Information domains that consist of the applications specific sub-functions or user activities(ASF/A), e.g. software maintenance, algorithms or hardware maintenance.

It is necessary for the systems specification to reflect the different security needs required of the diverse information domains. Although different information domains will exhibit similar or redundant security constraints and requirements during the initial identification activity, they will be identified for completeness sake. Subsequently, the convergent set of security requirements contained in the specification represents a reduced set of security requirements derived from this task. Accomplishment of the latter cannot be performed until individual information domain requirements are identified.

The notation used to discuss Information Domains Of (IDO):

- Applications Area (AA)
- Applications System (AS)
- Applications Specific Subfunction/Activities (ASF/A)

is thus, IDOAA, IDOAS, IDOASF/A.

B.2.1.0 Secure/Compartmented Prime Modes

B.2.1.1 Secure Operational Modes

The System Administrator (or Security Administrator if separate) will be responsible for using a combination of physical, procedural, hardware and software security to safeguard private, proprietary and classified information in a multi-project, multi-user enviroment. Classified operations will comply with DoD Directive 5200.28, Security Requirements for Automated Data Processing (ADP) Systems and derivative standards and guidelines.

B.2.1.2 Engineering Support Mode

CATALYST, when configured in the engineering support mode, shall support classified operation in the following compartmented modes:

Classified - A classified mode is one that requires that all users have a clearance for the highest information classification contained in the system and where the application is running in a dedicated/mandatory security status. Compartmented and need to know criteria will be in effect, since possession of a security clearance does not automatically provide access to all information cells.

- **System (AS or MCCS) Compartmented** - CATALYST is operating in the system compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:

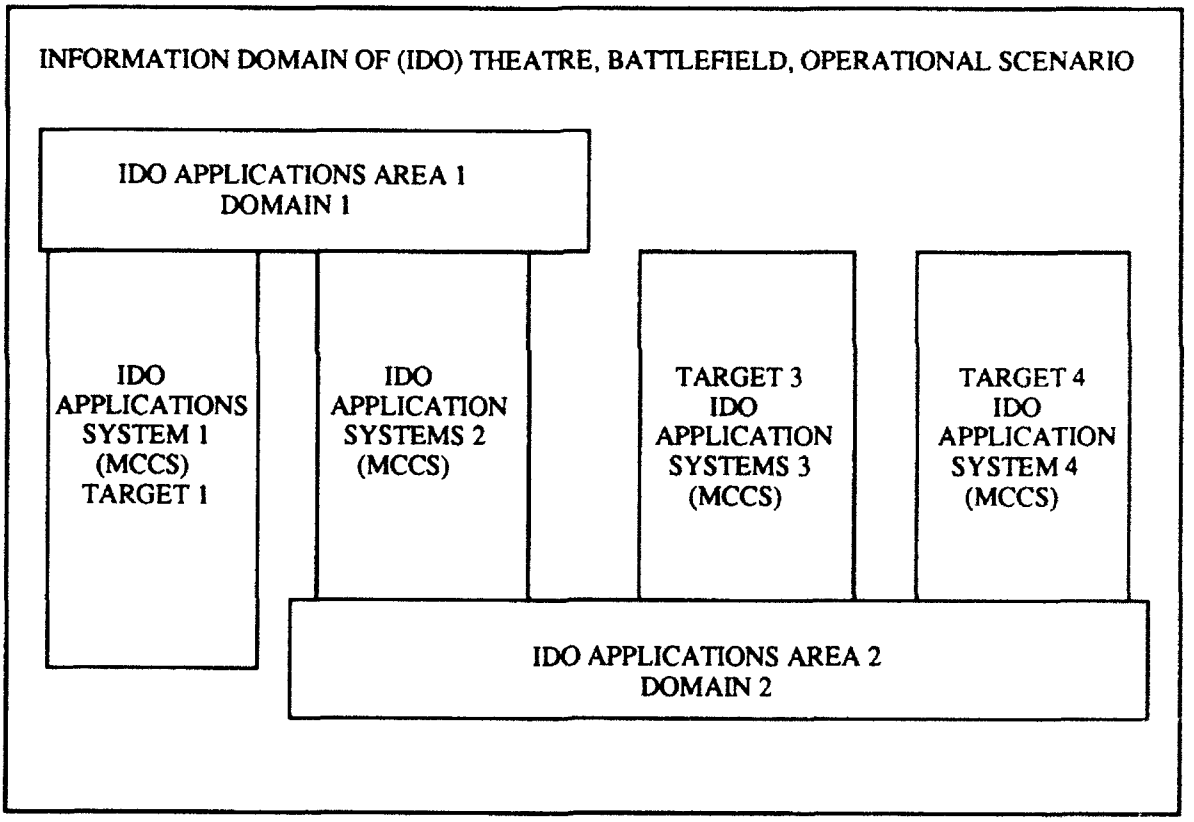
  a. A valid personnel clearance/access for just the information contained within a specific AS or mission critical computer system(MCCS) or

  b. A valid personnel clearance/access for the information contained relative to a specific system activity and domain(e.g. software maintenance, hardware maintenance, prototype analysis).

- **IDOAA Domain Compartmented** - CATALYST is operating in the AA domain compartmented mode(see Figure 7) when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:

  - A valid personnel clearance/access for just the information contained within a specific AA or
  - A valid personnel clearance/access for just the information contained within a specific AA domain(e.g. communications, fire control intelligence, air defense) or

- **AS Host Support Domain Mode** - CATALYST is operating in the AS host domain compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - a. A valid personnel clearance/access for the information contained within the host environment or
  - b. A valid personnel clearance/access for the information contained across a number(more than one) of host environments.
  - c. A valid personnel clearance/access for the information contained across a relative functional or object domain (e.g. algorithms, maintenance, error correction).
  - d. A valid personnel clearance/access for the information contained across a specific host and target system grouping(see Figure 5).



IDO--AA/AS CONCEPT & RELATIONSHIPS

Figure 7. IDO-AA/AS Concept and Relationships

Trusted Computer Base(TCB) Operation - A trusted mode is one that requires that all users have a clearance (different clearance levels are allowed) for their respective level of system access or operation, and where the application is running in a system high/ discretionary security status.

- **System (AS or MCCS) Compartmented** - CATALYST is operating in the system compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for just the information contained within a specific AS/MCCS or
  - A valid personnel clearance/access for the information contained relative to a specific system activity and domain(e.g. software maintenance, hardware maintenance, prototype analysis).
- **AA Domain Compartmented** - CATALYST is operating in the AA domain compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for just the information contained within a specific AA or
  - A valid personnel clearance/access for just the information contained within a specific AA domain(e.g. communications, fire control intelligence, air defense) or
- **AS Host Support Domain Mode** - CATALYST is operating in the AS host support domain compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for the information contained within the host environment or
  - A valid personnel clearance/access for the information contained across a number(more than one) of host environments.
  - A valid personnel clearance/access for the information contained across a relative functional or object domain (e.g. algorithms, maintenance, error correction).
  - A valid personnel clearance/access for the information contained across a specific host and target system grouping

B.2.1.3 Administrative Mode

CATALYST, when configured in the Administrative Support Mode, shall support classified operation in the following compartmented modes:

Classified

- **System (AS) compartmented** - CATALYST is operating in the system compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for just the information contained within a specific AS or
  - A valid personnel clearance/access for the information contained relative to a specific system activity and domain(e.g. status accounting, personnel staffing)
- **AA Domain Compartmented** - CATALYST is operating in the IDO theater compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for just the information contained within a specific AA (e.g. communications, fire control) or
  - A valid personnel clearance/access for just the information contained within a specific AA domain(e.g. message validation, message formats) or
- **AS Host Support Domain Mode** - CATALYST is operating in the AS host domain compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for the information contained within the host support environment or
  - A valid personnel clearance/access for the information contained across more than one host support environments.
  - A valid personnel clearance/access for the information contained across a specific host and target system grouping

Trusted Computer Base Operation

- **System (AS) Compartmented** - CATALYST is operating in the system compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for just the information contained within a specific AS or
  - A valid personnel clearance/access for the information contained relative to a specific system activity and domain(e.g. status accounting, personnel staffing)
- **AA Domain Compartmented** - CATALYST is operating in the domain compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for just the information contained within a specific AA (e.g. communications, fire control) or
  - A valid personnel clearance/access for just the information contained within a specific AA domain(e.g. message validation, message formats) or
- **AS Host Support Domain Mode** - CATALYST is operating in the AS support host domain compartmented mode when each user with direct or indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:
  - A valid personnel clearance/access for the information contained within the host support environment or
  - A valid personnel clearance/access for the information contained across more than one host support environments.
  - A valid personnel clearance/access for the information contained across a specific host and target system grouping

B.2.1.4 Training Support Mode

CATALYST users, prior to being assigned to operational or active engineering support systems will be required to undergo a training program in the use of, configuration management of, and policies and procedures associated with the environment. CATALYST, when configured in the training support mode, shall support different training configurations such as:

Classified Compartmented Training Mode - The classified mode is defined in section 1.2.1. CATALYST is operating in this mode when each user with direct and indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:

- A valid personnel clearance/access for training information contained within a specific AS or
- A valid personnel clearance/access for training information contained across a number of different AA or AS or
- A valid personnel clearance/access for AS host support information contained within a specific AA or
- A valid personnel clearance/access for AS host support information across a number of different hosts.
- A valid personnel clearance/access for the information contained across a specific host and target system grouping

Trusted Compartmented Mode - The trusted mode is defined in section 1.2.2. CATALYST, is operating in this mode when each user with direct and indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:

- A valid personnel clearance/access for training information contained within a specific AS or
- A valid personnel clearance/access for training information across a number of different AA or AS, or
- A valid personnel clearance/access for AS host support information contained within a specific AA or
- A valid personnel clearance/access for AS host support information across a number of different hosts.
- A valid personnel clearance/access for the information contained across a specific host and target system grouping

Sensitive/Initialization - The sensitive/initialization mode consists of training and exposure to actual CATALYST field configurations, scenarios and participation in live exercises implementing transition mechanisms. The information contained in this mode and its exposure to users, while not classified per se, requires that a CATALYST sensitive training environment status be declared and protected. CATALYST, is operating in this mode when each user with direct and indirect access to CATALYST, its peripherals, remote terminals, or remote host has the following:

- A valid personnel clearance/access for training information contained within a host environment
- A valid personnel clearance/access for training information across a number of different host environments
- A valid personnel clearance/access for training information across host and target environment combinations

B.2.2.0 Protection Support

CATALYST shall provide protection to information while it is compartmented or grouped within different user configurations. Information within the environment must be protected and disseminated on a need to know basis.

B.2.2.1 Discretionary

- Catalyst shall support discretionary protection for information within the environment on a need-to-know basis. Catalyst shall define and control access between named users and named objects in accordance with DoD 5200.28-STD DoD Trusted Computer Systems Evaluation Criteria.
- Catalyst shall identify an active user of the system through query of the underlying operation system. The operating system will be responsible for login procedures that include user identification, authentication or password. Where operating system responsibilities are precluded, responsibility for login may be delegated to a database or other software kernel for login procedures that may include, but not limited to, user identification, password or personal identification number (PIN). (ref. DoD 5200.28-STD para 3.3.2.1)
- Catalyst shall support the definition and enforcement of information access privileges explicitly by individual, by role, by group, and through identified information domains. (ref. SYSREQ-111.2c, SYSREQ-113.2f, g)
- Catalyst shall use the underlying capabilities of the operating system and database management system to restrict access to objects managed by Catalyst. Catalyst shall support the following access privileges by object, as defined by NCSC-TG-003:

- read
- write-append
- write
- delete
- execute
- control
- control with passing ability
- null (no access)

- Catalyst shall provide the ability for users with control privileges to specify, for each object, authorized users and their access privileges and unauthorized users. The discretionary access control defaults shall protect objects from unauthorized access.
- Catalyst shall support the definition of information domains and the association of objects to one or more domains. Information domains may overlap and all objects do not have to be assigned to a domain.
- Catalyst shall provide the ability for users with control privileges to specify, for each information domain, the authorized users and their access privileges and unauthorized users.
- Catalyst shall support audit mechanisms to account for security-relevant events affecting discretionary security. (Ref. DoD 5200.28-STD para 3.3.2.2)
- Catalyst shall support automatic termination of a user session based upon an extended period of user inactivity, not to exceed 15 minutes.

B.2.2.2 Mandatory

- Catalyst shall utilize the underlying facilities of the TCB to provide mandatory access control during classified operations. Catalyst shall not violate the mandatory security policy being enforced by the TCB. (Ref. DoD 5200.28-STD para 3.3.1.4)
- Catalyst shall identify the security level of an active user of the system though query of the underlying operating system of the Trusted Computing Base. The operating system will be responsible for maintaining the security levels of users. (Ref. DoD 5200.28-STD para. 3.3.1.4 and 3.3.2.1)
- Catalyst shall support the tagging of objects managed by Catalyst with a sensitivity level (e.g., security classification level) consistent with the security policy of the installation. The sensitivity labels shall be

consistent throughout Catalyst objects. The sensitivity labels shall be used as the basis for the mandatory access control provided by the underlying TCB. Reclassification of sensitivity labels shall only be accomplished by authorized users. (ref. DoD 5200.28-STD para 3.3.1.3)

- Catalyst shall support and use the underlying capabilities of the operating system of the Trusted Computing Base to restrict access to objects managed by Catalyst by sensitivity level (e.g., security classification level) according to the mandatory access control security policy. Catalyst shall define and control access between named users and named objects. While Catalyst may employ aggregate methods of specifying access control (i.e., by role, group or information domain), a granularity of a single user and a single object shall also be supported. (Ref. DoD 5200.28-STD para. 3.3.1.4)
- When Catalyst displays, prints or exports an object to any multi-level I/O device, the sensitivity label associated with the object shall also be displayed, printed or exported and shall reside on the same physical medium, in the same form (i.e., machine readable or human readable), and in accordance with security policies. Exported sensitivity labels shall accurately and unambiguously represent the Catalyst internal labels and be associated with the information being exported. Single level paths do not require sensitivity labels. (Ref. DoD 5200.28-STD para 3.3.1.3.2.1 and 3.3.1.3.2.3)
- When Catalyst exports or imports objects over a multi-level communications channel, the protocol used shall provide for the accurate and unambiguous pairing between the sensitivity labels and the associated objects that are sent or received. (Ref. DoD 5200.28-STD para 3.3.1.3.2.1)
- All authorizations to information contained in a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from Catalyst's pool of unused storage objects. No information, including encrypted representations of information produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. (ref. DoD 5200.28-STD, para 3.3.1.2)
- Catalyst shall support the sanitization of information by removing objects above a certain classification level from printed material or by exporting selected information in accordance with an installation's security policy.
- Catalyst shall support the network and long haul communication of objects managed by Catalyst using the underlying trusted communications mechanisms of the Trusted Computing Base. Catalyst shall support use of public and private key encryption mechanisms and those compliant with the U.S. Data Encryption Standard (DES).

- Catalyst shall support audit trail mechanisms to account for user actions affecting mandatory security, including the following:
  - Use of identification and authentication mechanisms,
  - Introduction of objects into a user's address space (e.g., open a file, initiate a program),
  - Creation, access, modification or deletion of objects,
  - Modification of object sensitivity levels,
  - Import of non-labeled or erroneously labeled data,
  - Override of human-readable sensitivity markings,
  - Changes in security defaults or auditing level,
  - Changes in TCB or network configuration or connectivity,
  - Actions taken by specially-privileged users (e.g., system administrator, security administrator), as well as other events defined by security policy. (Ref. DoD 5200.28 para. 3.3.2.2)
- Catalyst shall support automatic notification of security-relevant events according to an organization's security policy. (Ref. DoD 5200.28 para. 3.3.2.2)
- Catalyst shall support use of removable storage media for all of its stored information.
- Catalyst shall provide utilities to adequately clear non-volatile storage according to security procedures.

B.2.2.3 Submode

CATALYST shall support operation in a number of different configurations intended to support integrity of activity, maintain operations and mission effectiveness while in any of the following submodes:

Single User - CATALYST shall support users with dedicated terminals/workstations or other dedicated assets. In this mode CATALYST shall identify an active user of the system through query of the underlying operating system or database. The operating system shall be responsible for log in procedures that include user identification, authentication or password. Where operating system responsibilities are precluded, responsibility for log in may be delegated to a database or other software kernel for log in procedures that include, but not limited to, user identification, password or personal identification number(PIN).

Multi-User - CATALYST shall support users that will operate in a multi-user (shared assets) environment with compartmented domains. In this mode CATALYST shall identify an active user of the system through query of the underlying operating system or database. The operating system shall be responsible for log in procedures that include user identification, authentication or password. Where operating system responsibilities are precluded, responsibility for log in may be delegated to a database or other software kernel for log in procedures that include, but not limited to, user identification, password or personal identification number(PIN) and terminal/workstation user identifier.

Network - CATALYST shall support users in a networked environment containing dedicated and shared assets. The environment is expected to have CATALYST access at a number of remote or local area entry points via dedicated and shared terminals. In this mode CATALYST shall identify an active user of the system through query of the underlying operating system or database. The operating system will be responsible for log in procedures that include user identification or password. Where operating system responsibilities are precluded, responsibility for log in may be delegated to a database or other software kernel for log in procedures that include, but not limited to, user identification, password, personal identification number(PIN) or network PIN, or network verification schema. CATALYST shall avoid or minimize cascade problems to the extent possible.

Fault/Diagnostic/Maintenance - When in this mode, CATALYST designated users with direct and indirect access to CATALYST, its peripherals, remote terminals, or remote host shall be prevented from making disclosures to protect:

- The unauthorized transition to an active state
- The unauthorized and inadvertent release of information
- The unauthorized query of system states(MCCS's) and components thereof
- The unauthorized query of system(MCCS) readiness and configuration
- The unauthorized changes of configurations and components thereof.

B.2.2.4 Recovery

CATALYST shall use the underlying capability of the operating system, data base kernel and configuration status accounting to provide a recovery capability to enable mission or support continuation. In addition to the other recovery requirements in the specification the following shall also apply:

- CATALYST shall provide the ability to query configuration status accounting and effectively transition from a degraded or lesser operational capability state to a higher operational capability state.
- CATALYST shall support automatic coordination and configuration between the system administrator and the security administrator.
- CATALYST shall support the automatic dissemination of recovery information and configuration control information to appropriate and required system managers (i.e. security officer, system administrator, configuration manager, AS host support supervisor).

B.2.3.0 Configuration Management

B.2.3.1. Secure Configuration Management

CATALYST shall be responsible for providing configuration management of its trusted system and trusted system components. CATALYST trusted configuration management(TCM) shall consist of controlling, identifying, accounting for, and auditing of all changes made to the CATALYST TCB during its design, development, maintenance, pre-deployed and deployed states. The security CM measures shall be in conformance with National Computer Security Center, Configuration Management in Trusted Systems, NCSC-TG-006, Version 1, 28 October 1988.

CATALYST trusted configuration management(TCM) shall maintain control of its environment throughout its life cycle, ensuring that the system in operation is the correct one, implementing the correct security policy.

To insure that CM changes take place in an identifiable and controlled environment, and that the changes do not adversely affect any properties of the system, CATALYST TCM shall:

- Maintain control of changes to the design specifications
- Maintain control of data to other parts of the environment affecting it
- Maintain control of changes to the implementation documentation (i.e. user's manuals, operating procedures)
- Maintain control of changes to test fixtures
- Maintain control of changes to test documentation
- Maintain control of changes to the software(i.e. source code, object code)
- Assure consistent mappings between all documentation and code associated with the trusted computer base and trusted data base.
- Maintain the integrity of COTS tools
- Provide tools for comparisons of newly generated trusted computer bases
- Maintain under strict CM control, any tools used to provide CM to CATALYST itself
- Protect from unauthorized modification or destruction master copies of all material used to generate or support the TCB
- Not preclude the implementation of TCM at levels higher than B3.

The CATALYST environment consists of a diversity and variety of hardware and software components, COTS products, network elements, peripheral devices, physical and electronic security measures and products, remote devices and terminals, and remote hosts. CATALYST shall develop and have its own customized CATALYST Ratings Maintenance Plan (CRAMP), consistent with the RAMP requirements of NCSC.

The CRAMP shall for:

1. COTS equipment and products be in conformance with the NCSC Ramp requirements and outlines
2. CATALYST unique products and developed software be in conformance with the NCSC Ramp requirements and outlines
3. CATALYST environment configurations (i.e. combinations of 1. and 2. above) have a customized/tailored RAMP supportive of CATALYST policies and procedures, that do not violate the integrity of the individual RAMP plans of 1. and 2.
4. All design and analysis tools claiming to have a CM capability, verify the extent to which CM is formally integrated into the tool(s), and into the design baseline in which the tool(s) is/are used to support TCM implementation, policies and procedures.

B.2.3.2 Certification

CATALYST shall support, through its TCM capability, the following:

- Certify that the current software baseline is consistent with its documentation and configuration (i.e. establish mapping relationships)
- Certify that security policies and procedures are not being violated
- Certify that the network does not have any covert channels
- *Certify the integrity of the network(i.e. no cascade situation exists)*
- Certify and verify that no unauthorized user can create changes to the system, its configuration or software baselines without being subject to a formal approval and change process
- Certify and verify the integrity of CCB members and their authority
- Certify and verify "electronic signatures" required to authorize environment changes.

CATALYST shall certify and enable the distribution of CCB information changes and implementations electronically (i.e. in a paperless mode).

TCM represents an added measure of protection for CATALYST. It should not be depended on as the sole vehicle or system to provide system security relative to CM. However, it should be independent of the secure operating system's ability to provide the trusted CM function as well as it can, and in the event of secure operating system failure. TCM shall provide protected configurations without the availability of secure operating systems or kernels. Protected configurations shall be comprised of but not limited to:

- Trusted data bases
- Network encryption devices
- Protocol and other network related encryption devices and schema.
- Secure terminal equipment compliant with U.S. Data Encryption Standards
- Physically secured configurations

Other commercial data encryption standards may be used subject to review of the particular encryption approach and in the absence of a Government standard for the particular product.

B.2.4.0 Administration/Responsibilities

In a trusted or classified environment CATALYST shall provide for administrative and assignable responsibilities, and rules for the following:

- A separate and identifiable TCM operational capability from that of the system administrator
- A well defined configuration control board(CCB) with roles, authority and membership for the purposes of administering and enforcing TCM
- A trusted configuration manager separate from the system administrator, with duties and responsibilities well defined
- A defined set of facilities to enable the execution and implementation of TCM. The facilities shall be isolatable from the system administrators facilities.
- An established and published set of policies, procedures, and instructions for all CATALYST users identifying their respective domains of operations and capabilities.

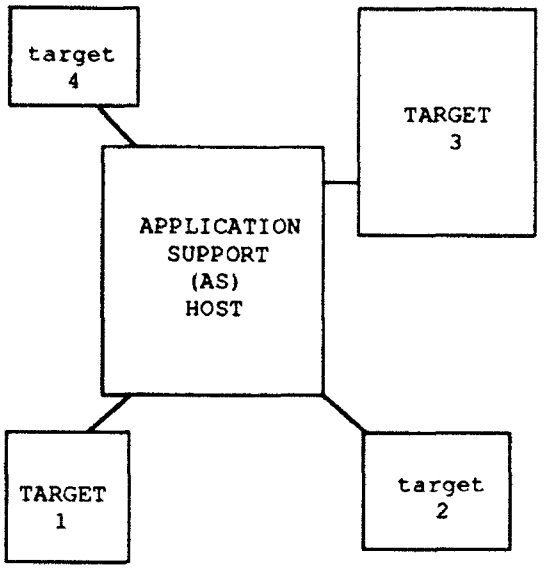
B.3 Rationale/Background

As a systems engineering environment, CATALYST is expected to contain much information directly relatable to requirements, doctrine and mission performance both within specific information domains and across them. Thus, the information sensitivity and insight that can be obtained from such an environment is critical. Furthermore, the ability to extrapolate to, and establish a correlation of other sensitive views within an application area, from seemingly unclassified information cells, represents a significant potential for compromising those systems.

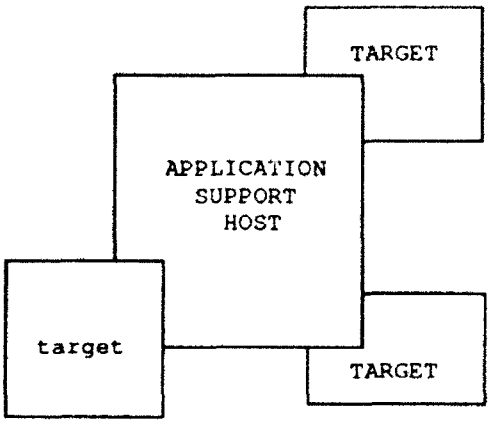
To insure that mission operation and effectiveness is not compromised, CATALYST must have the ability to compartment and limit the views that are possible to unauthorized individuals, and users that do not have a need to know.

Information domains of applications areas will vary in scope and magnitude depending on the particular branch of service(i.e. Air Force, Army, Navy or Marine Corps), see Figure 7.

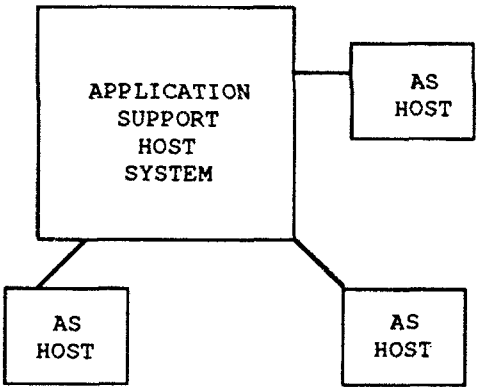
- An applications area is just as the name implies, a major element of the battlefield representing such areas as air defense, intelligence, combat support services, artillery, electronic warfare, class of ship, or a tactical wing.
- An applications area domain is a common sub-element within the applications area such as a particular type of intelligence, fire mission algorithm, or electronic warfare jamming frequency algorithm.
- An AS is the actual system, aircraft, or ship within an AA. It is the same as the target system from a AA perspective. From an AS support host perspective it is not necessarily the same configuration(see target system).
- An AS support host is the system supporting an AS, and responsible for generating new versions of software or making fixes to systems in the field. The AS support host interacts with a target system it is making a fix for or solving a problem associated with the particular AS, see Figure 8.
- An AS support host system is a AS support system given an added or specialized responsibility whereby this system transitions tools, certifies tools, and manages the development environments used by the other support centers that are actively supporting target systems. The AS support host does not have any target systems associated with it, but instead supports other AS support systems.



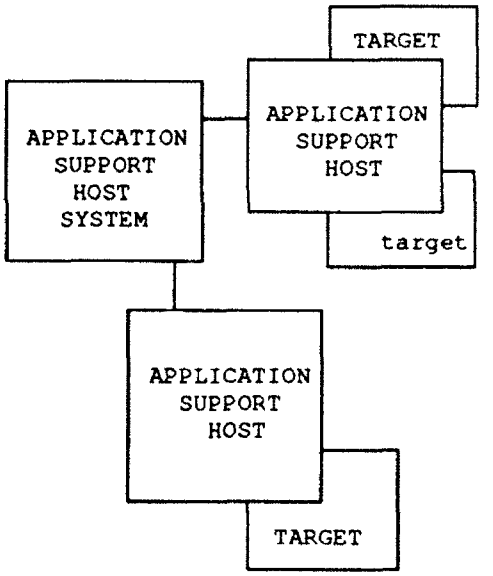
Current Environment: ASH/TARGET
have unique assets



Desired environment: common asset
ASH/TARGETS



ASHS/AS HOST
relationship



ASHS/ASH/TARGET overview

Figure 8. Configurations of Hosts and Target Systems

B.4 Requirements Considerations

It is envisioned that with the security element there will be required per the NCSC requirements the following documents:

- CATALYST Security Policies & Procedures Manual(CSPPM)
- Trusted Facility Manual(TFM)
- CATALYST Ratings Maintenance Plan(CRAMP)
- Configuration Management Plan(CMP)
- Trusted Configuration Management Plan(TCMP)
- Ratings Maintenance Plan(RAMP)

These documents may be required as separate documents, or as combined ones (e.g. CRAMP could be an appendix of a CMP).

C. Task 3 - Security Architectures: An Approach

The numerous applications and extensive set of requirements that CATALYST is expected to support necessitates that an open architecture be supported within the CATALYST environment. A systems engineering environment such as CATALYST provides the essential coupling (building blocks) between the user requirements and the ensuing design domains; between the conceptual views of the user and implementation prototypes; and between the synthesis and allocation domains. Critical linkages must also be established between the system and its elements (i.e. hardware, software, firmware). The linkages in turn enable interfaces and viable bilateral communications paths to exist that subsequently become a very important part for resolving problems whenever and wherever they occur in the life cycle. Thus, for effective architectures to exist, requirements and their relationships to each other must first be established, representing a set of building blocks upon which the architecture is based.

This task focused on deriving security architectures that could be used to support the CATALYST environment. Prior to architectural definition, requirements identification and refinement must be accomplished. During the SECD contract period this was accomplished. The concurrent security and requirements analyses tasks performed have established the foundations for the identification of a feasible security architecture. Subsequent SECD implementation initiatives can definitize the security architecture required for CATALYST. Thus, the concurrent nature of tasks supported the identification of generic building blocks used to support a security architecture, along with a brief summary of a systems security engineering process(SSE). An SSE process must first be defined and underway during the initial stages of concept definition, to effectively develop a

security set of requirements and guidelines. The latter requirements and guidelines can then be used to:

- Identify supporting architectures
- Provide risk mitigation insight
- Provide threat identification
- Establish vulnerability prioritization
- Identify candidate measures
- Refine the initial requirement set.

This iterative SSE process enables security to mature within the domain that CATALYST is expected to support and become an integral part of. The latter is the preferred approach instead of treating security as a separate activity levied directly on top of the system set of requirements. This iterative approach results in an overall set of cohesive requirements creating less requirements instability.

An initial set of requirements and issues has already been identified in two areas: in the SECD specification[4] and in the technology assessment Task 2 report. The issues raised in these two documents can be summarized as follows:

- Imposition of security on CATALYST bears an added weight, cost and complexity.
- Supporting security technologies are maturing and still undergoing change
- The existence of security domains(i.e. operating system, data base, network) together with existing technology require evolutionary and incremental implementation approaches.
- The full interaction of security domains has yet to be identified(e.g. covert channels may be found to exist).

Furthermore, overlaying the security requirements on CATALYST imposes architectural constraints that must be tempered by the emerging mission support roles that will continue to be defined for CATALYST. Item C in particular, will have an impact on the architectural views and approaches needed by CATALYST.

---

4 System Specification for the CATALYST System, SSS-90-001: 3 August 1991, Revision 02.00 : 1991/05/29 00:00:00; Rome Laboratory: Contract No. F30602-90-C- 0021

C.1 Major building blocks

The major security building blocks required to support a trusted CATALYST environment architecture are:

1. Secure operating system(SOS)
2. Trusted data base(TDB)
3. Secure network
4. Compartmented Mode workstation(CMW)
5. Trusted configuration management(TCM).
6. A physically protected environment
7. Complete and supporting documentation methods and procedures, etc. for the above items.

It is recognized that each of the identified building blocks can be used to implement security in isolation or independent of the others(e.g. a SOS can be used without a TDB). However, employment in this manner, from a security standpoint, leaves much to be desired[FAD91]. The most viable architecture is one that consists of or uses all of the different building blocks. The building blocks themselves are generic enough in structure in that they enable a variety of CATALYST configurations to coexist(i.e. single user platforms, multi-user platforms, networks and distributed network elements). The building blocks are thereby capable of supporting a variety of different architectures. In certain applications one generic building block can be replaced by another(i.e. co-located and isolated platforms can be supported by a physically secure cell instead of a SOS if the proper procedures are employed).

In some design representations(e.g. a distributed one), some building blocks provide greater architectural integrity than others. In the distributed case, having a secure operating system at each distributed processing element affords greater security protection than a trusted database element. However, utilization of both a SOS and a TDB in a distributed architecture provides greater protection than using just one type of generic block.

The differences and complexities in trusted types and information security classification levels dictate that all of the different generic blocks be employed within any given architecture unless otherwise specifically precluded. Use of as many different types of building blocks as possible insures the highest level of trustedness. This represents a safe approach when in doubt. What remains to be determined in complex architectures is the overhead processing incurred and system response when each element within a design representation contains one of each type of building block(i.e. one each of items 1 through 4). Is the security

overhead acceptable and within system performance tolerances? The interactions between SOS, TDB, secure network, etc. in a complex design remain to be instrumented and measured. Similarly, covert channel analysis in a distributed database implementation, may prove to be difficult to assess and verify.

C.2 System Security Engineering Process

However, notwithstanding the existence and availability of security building blocks, a viable CATALYST architecture demands that the systems engineering performance and requirements needs be supported by and integrated with the security requirements domain. Furthermore, in the area of security few techniques are available to provide the analytical and quantitative support for exacting requirements in environments with the complexity of CATALYST. Thus, to provide a proper framework for derivation of system security architectures for subsequent integration into the systems design process, a system security engineering(SSE) process must be developed. The SSE process complements and supports the CATALYST system engineering concept definition activities. To be effective, the process must be well-defined and initiated concomitantly with the early SECD requirements synthesis tasks. Additionally, the resulting security architectures must be evaluable and justifiable if security is to be recognized as an essential component of the environment.

One such approach, of potential value to SECD effort that can be utilized as a security baseline process is AT&T's Systems Security Process. The process was originally designed for use on the Strategic Defense Initiative(SDI) Systems Engineering and Integration contract[CHA87][WEI91]. The AT&T process was established as a formal implementation of Mil-Std 1785, System Security Engineering Program Management Requirements. It has also been subsequently applied on AT&T products and services. Some highlights and summaries of the process will be presented:

The objective of the SSE process was to derive a cost-effective system security architecture and to integrate it into the system design process. The resulting architecture was to be evaluable and justifiable. The AT&T SSE process was also intended to provide a well-defined framework that could be used to iteratively support security requirements evaluation and justification. AT&T recognized the need for such an environment and process as a result of their quantifiable work and means of establishing formal measures in communications networks, systems and protocols. It was felt that they strongly needed a representation of a uniform process for providing analytical support for system security requirements.

The SSE consists of a security vulnerability analysis(SVA), security requirements integration process and automated tool support. SVA in turn is based on risk management theory, structured analysis, AT&T's fault tree constructs used in reliability engineering, and internally derived empirical risk formulas. The goal of SSE is to identify security architectures that fall on the curve of optimal reduction of security risks for applied security dollars. Ten steps are involved in SSE:

1. Baseline architecture identification
2. Threat identification
3. Threat analysis and decomposition
4. Risk assessment
5. Prioritization of vulnerability
6. Identification of candidate safeguards
7. Safeguard trade-off analysis
8. Security architecture selection
9. Security architecture integration
10. Iteration

An SVA model is required so that individual activities within steps 1 through 10 can be mapped into the specific elements of the model. The model consists of the following components:

- Baseline requirements
- Baseline architecture
- Adversary threats
- System valued assets
- Configuration management & version control
- Prioritized threats
- Threat logic trees
- Threat database
- Critical functions database
- Critical information elements database
- Security safeguard & countermeasures database
- Security policy

Step 1 consists of defining an architecture from a performance perspective, with system security characteristics(if any) interspersed among other system design elaborations. SSE should commence from the very beginning of system definition activity.

Readers are referred to [WEI91] for elaboration of the ten steps.

The model recognizes that the probability of attack on a system is very difficult, if not impossible to estimate since:

- Adversaries are unknown, thus it is very difficult to predict the types, frequencies and degrees of motivation.
- Adversary attributes are unknown since the adversaries' capability, disposition and resources are not known.
- Unknown futures, since time favors the attacker's ability to exploit weaknesses, technology or opportunities.

Thus, the ability to predict when an attack will occur cannot be accurately determined. However, AT&T has employed a risk formula that does not require so accurate an assessment of the adversary mindset. The model's formula assumes the worst case scenario of an adversary that applies available resources intelligently. Thus, there is no need to suppose specific adversaries and assess individual motivations. The formula is based on a system weighted penalty(SWP), which enables consideration for severe vulnerabilities that are difficult to exploit today, with the assumption that their presence may represent a future threat.

The model is iterative in nature thus allowing for the ability to update threats, capture architectural variances, and vulnerability changes. Strict configuration management and version control of the databases, threat logic trees, and outputs of the SVA model(i.e. security vulnerabilities, security requirements and architectures, and security policy impacts) must be maintained to track system architectural shifts and allow "what if" analyses. Additionally, configuration management provides the traditional ability to return or trace back to previous baselines.

To effectively and efficiently allow the capture and analysis of information, automated tools should be employed to facilitate this aspect of the process. AT&T Bell Laboratories has developed a prototype Automated SSE Toolset(ASSET). The tool runs on an AT&T 630 Multi-Tasking Graphics terminal that supports the following features:

1. Threat logic tree generation and management
2. Automated risk calculation and recalculation capabilities
3. Risk parameter and subparameter input forms
4. Automated report generation of hardcopy threat logic trees and summary reports
5. Automated threat and safeguard databases
6. Integrated configuration management
7. On-line help capabilities

Future capabilities are planned for ASSET that include:

1. Critical risk path highlighting for threat logic trees
2. Generation of wall chart threat logic tree reports
3. Incorporation of threat subtree libraries
4. Automated safeguard trade-off analyses
5. Integrated cost models
6. Integrated system modeling capabilities
7. Support for non-expert users.

This process is intended to provide analytical support for the identification and establishment of security requirements. It is intended to provide engineering and risk management principles to administer security resources effectively. It is to be expected that as use is made of the tool, broader and more extensive problem sets can be undertaken.

C.3 Pragmatic architecture

The current state-of-the-practice can provide B1 through B3 levels of trustedness with commercial-off-the-shelf(COTS) products by such major vendors as DEC, SUN, IBM, Oracle, Informix and Verdix, amongst others. CATALYST networks(Figure 9) and CATALYST frameworks(Figure 10) can be supported by the architectural building blocks identified previously in this report. Where the state-of-the-practice begins to encroach on the state-of-the-art is in establishing the complex networks using the CATALYST framework architecture.

combinations of complex structures such as those identified in Figures 9 and 10 have not. Much more extensive assessments in network access, covert channels[BAD91][FIT91] and polyinstantiation would have to be performed to gain trusted levels of B3 or higher[DEN91]. The CATALYST environment can be used to gain much information in the area of trustedness of complex networks.

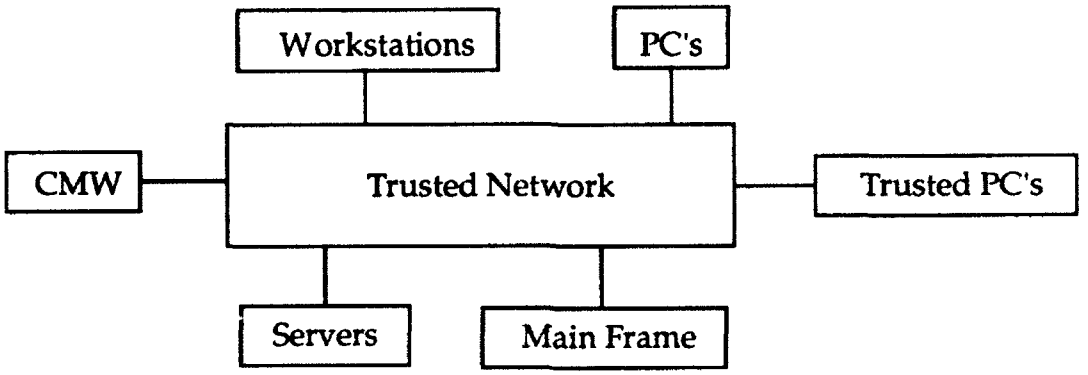


Figure 9. CATALYST Network

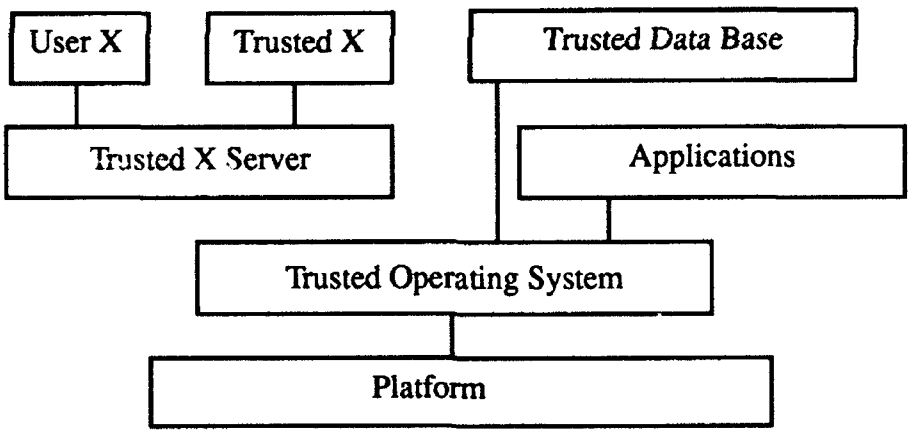


Figure 10. CATALYST Framework

One generic building block omitted from the list is a trusted X windows block. At this time a trusted X windows system[EPS91] is considered to be the weak link in the structure, notwithstanding the fact that platform vendors currently undergoing Government certification have indicated that they intend on using X windows as the basis for their trusted windowing system. The concern at this time is that the X philosophy promotes cooperation among applications,

undergoing Government certification have indicated that they intend on using X windows as the basis for their trusted windowing system. The concern at this time is that the X philosophy promotes cooperation among applications, including the sharing of data and resources. Trusted systems require degrees of isolation which is in fundamental conflict with the X windows approach of sharing resources. It is this temporary weak link that reinforces the use of all of the architectural building blocks identified at each processing element within the network. However, adoption of the approaches identified in [EPS91], provides the basis for building trusted X products at the B3 level within the next 2 to 3 years. While availability of a trusted X windows generic block has yet to attain a COTS designation, major implementation problems or barriers are not foreseen in this area.

C.4 Trusted System Development Methodology

One other element that will complement the SSE process and architectural definition task is the establishment of a trusted system development methodology. The approach has foundations and merit as revealed in the related Strategic Defense Initiative(SDI), "A Trusted Software Development Methodology(TSDM)". The approach was employed by the Systems Engineering and Integration contractor, General Electric[SDI90], as a task defining trusted systems requirements and architectures for the SDIO Program Office. The methodology covers such areas as trust principles, compliance criteria and trust classes. It is intended to identify measurable principles and methods for determining levels of trust and increasing the trust of new and existing strategic defense systems software. The focus of the SDI methodology is on software protection and integrity due to its complexity and volume.

The TSDM is essentially an SDI customized effort, using as its foundations NCSC trusted criteria, guidelines and requirements per DOD 5200.28 [NCS85c]. It develops its own set of trusted levels, identified as T1, T2, T3, T4, and T5 that correspond somewhat to the NCSC trusted levels of C1 through A1. A section of the methodology document is intended to provide guidelines for determining how to define an architecture in a manner that insures the integrity of those portions of the architecture that are deemed "critical". However, this section of the document has yet to be produced, and a draft version is scheduled for some time in second quarter FY 1992.

The variations and priorities in trusted levels are driven in part by such elements as software reuse, prototyping, formal specifications, requirements integrity and formal code audits specific to SDI and their environment needs. The methodology document similar to NCSC documentation also contains a methodology applications guidelines section. The latter contains insight on how to use the principles established and criteria classes, how to apply the

methodology to new versus existing software, how the methodology applies to prototyping efforts, and a summary of the approaches that are being developed for allocating trust to a software architecture.

The methodology examines issues related to the Software Engineering Institute's process maturity methodology for possible influences on the trusted software methodology. A number of areas are identified that can assist in assessing the completeness of the trust principle compliance requirements, and modifications thereof as a consequence of utilizing the SEI process maturity questionnaire[SEI91]. The SDI Trusted Software Development Methodology is an on-going and maturing effort. It was recognized that such an activity was needed early in the requirements definition phases of the program in order to establish a viable security program with the criticality and complexity of SDI and the information that required protection.

While emphasis of the SDI methodology was on software, many aspects of it are directly relatable to a system engineering methodology and environment relative to security issues. Prototyping and reuse in the CATALYST environment are just as critical, if not more so, than its counterpart in the SDI world. The importance of a formal systems engineering prototype(i.e. one supported by an executable specification) cannot be underscored. System performance issues, requirements integrity, traceability and allocation are very critical areas that affect all subsequent life cycle activities. The ability to examine and trade off the latter via formal prototypes can provide much insight into risk mitigation approaches.

Similarly, reuse takes on an added dimension at the systems engineering level of abstraction; and becomes even more critical at this level than at the software level of abstraction. Reuse must be considered in the context of design, architecture, specifications, algorithms, hardware and software. Similarly, reuse libraries at the system engineering level can take on added complexity and depth. In essence, the CATALYST environment will have to customize and develop its own trusted methodology as these other programs have done.

Interfaces/Standards - With respect to interface standards that CATALYST must conform to, no major obstacles can be identified at this time based upon the following:

- All major workstation vendors are supporting both X windows and UNIX
- Database developers are using SQL languages and industry standards
- Network protocols used are TCP/IP
- With the exception of a trusted X certified implementation all other product building blocks have been certified or are undergoing certification with the Government(see section VI A). By December 1992 additional product offerings will be nearing certification.
- With the exception of a few proprietary architectures, all major vendors, e.g. IBM, DEC, HP, Sun, Informix, Oracle, etc. can provide security products at the B level of trustedness(see Table 1).
- The need for new interface standards can be addressed once an environment is identified using the NIST Reference Model for Frameworks[NIS91], and the SECD process model in particular.

One area of security concern that is still considered weak is configuration management. Global configuration management to the extent required by CATALYST will demand innovative and complete approaches. COTS Tools and environments for the most part have ignored CM and its criticality. This is particularly evident in computer-aided-software-engineering(CASE) tools, where CM has not been addressed adequately. A requirement for CM in CASE has always existed, particularly for integrated CM. Yet vendors have ignored the need for such. With trusted configuration management a must requirement at higher trust levels[NCS88c], major compromises in security can be anticipated unless the issue is addressed very early and extensively in CATALYST's life cycle. The problem is exacerbated by the lack of CM automation support into the environment and tools.

Summary

Three key components or activities have been identified, that are required to effectively define and establish a viable CATALYST architecture:

1. Systems security engineering process
2. Trusted development methodology
3. Baseline architectural building blocks

Development of 1 and 2 can be concomitantly supported with activities involving the generic building blocks of 3. Architectural baselines can be structured early in the security process for subsequent evolution and refinement. Furthermore, these baselines can be used to measure and quantitatively assess the impact on performance and cost as a consequence of imposing security on a system. New metrics and measurands can be identified that can be used to establish risk mitigation strategies alongside system integrity and trustworthiness.

Any security initiative undertaken should consist of all three key components. The demand for near term system implementations can be effectively supported at the B2 level via the building blocks as they exist today. Levels of trust at the A level will not be forthcoming until the latter part of this decade(1995-1997). Furthermore, other evolutionary and incremental approaches can be on-going to provide further trusted extensions and refinements in a domain where the CATALYST environment and concepts represent the state-of-the-practice, state-of-the-art and beyond, as a unique initiative in the systems engineering arena at this time.

VII. Bibliography

[BAD91] Badger, L., "Covert Channel Analysis Planning for Large Systems", Proceedings of the 14th National Computer Security Conference, Oct. 1991

[BEL73] Bell, D., and La Padula, L., "Secure Computer Systems: Mathematical Roundations and Model", Mitre Report MTR 2547, Vol. 2, Nov. 1973

[CEN91] Chilton's Electronic News, September 30, 1991, Page 14, "Beaver Computer Corporation"

[CHA87] Chancer, R., Charney, J., Kolchmeyer, P., and Mayer, V., "Security Assessment of Services, Products and Architectures", AT&T Bell Laboratories Technical Memoranda 55131-87008.01TM, Oct. 8, 1987

[DEN91] Dennison, M.W., "Practical Models for Threat/Risk Analysis", Proceedings of the 14th National Computer Security Conference, Oct. 1991

[DOT89] Department of Transportation Federal Aviation Administration, "FAA Automated Information Systems Security Handbook", No. 1600.54B, Feb. 7, 1989

[EPS91] Epstein, J., Picciotto, J., "Trusting X: Issues in Building Trusted X Window Systems or What's Not Trusted About X", Proceedings of the 14th National Computer Security Conference, Oct. 1, 1991

[FAD91] Faden, G., "Reconciling CMW Requirements with Those of X11 Applications", Proceedings of the 14th National Computer Security Conference, Oct. 1991

[FCW91a] Federal Computer Week, September 2, 1991, Page 3, "Key Encryption Standards"

[FCW91b] Federal Computer Week, June 10, 1991, Page 37, "Encryption Standards"

[FIT91] Fitch, J.A. and Hoffman, L.J., "The Cascade Problem: Graph Theory Can Help", Proceedings of the 14th National Computer Security Conference, Oct. 1991

[FLI89] Flink, C.W., and Weiss, J.D., "System V/MLS Labeling and Mandatory Policy Alternatives", Proceedings of the 1989 Winter USENIX Conference, Feb. 1989

[FUT91] Futcher, D.A., Sharp, R.L. and Yasaki, B.K., "Building a Multi-Level Secure TCP/IP", Proceedings of the 14th National Computer Security Conference, Oct. 1991

[GCN91] Government Computer News, September 2, 1991, Page 10, "NIST"

[HEM86] Hemdal, G., "In Search of a New Architecture", Network Magazine, Nov. 1986

[JIA91a] Joint Integrated Avionics Working Group (JIAWG), WPAFB, "Software Engineering Environment(SEE) System Security Requirements and Issues Specification", Specification No. JW90-4AA6AB-012-01-01, 9 July 1991

[JIA91b] Joint Integrated Avionics Working Group (JIAWG), WPAFB, "Software Engineering Environment System (SEES) Security Policy", Specification No. JW90-4AA6AB-012-02-02, 1 July 1991

[KEV91] Kevin, B., "Integrating B2 Security Into A UNIX System", Proceedings of the 14th National Computer Security Conference, Oct. 1991

[MAY91] Mayfield, T., Boone, J., and Welke, S.R., "Integrity Oriented Control Objectives: Proposed Revisions to the Trusted Computer Systems Evaluation Criteria(TCSEC), DOD 5200.28-STD", IDA Document D-967, Institute for Defense Analysis, 1991

[NCS85a] National Computer Security Center, "Password Management Guideline", CSC-STD-002-85, April 1985

[NCS85b] National Computer Security Center, "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements", CSC-STD-004-85, June 1985

[NCS85c] National Computer Security Center, "Trusted Computer System Evaluation Criteria", DOD 5200.28-STD, Dec. 1985

[NCS85d] National Computer Security Center, "Personal Computer Security Considerations", NCSC-WA-002-85, Dec. 1985

[NCS85e] National Computer Security Center, "Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments", CSC-STD-003, 25 June 1985

[NCS87a] National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria", NCSC-TG-005, 31 July 1987

[NCS87b] National Computer Security Center, "A Guide to Understanding Discretionary Access Control in Trusted Systems", NCSC-TG-003, 30 September 1987

[NCS88a] National Computer Security Center, "A Guide to Understanding Audit in Trusted Systems", NCSC-TG-001, Version 2, June 1988

[NCS88b] National Computer Security Center, "Computer Security Subsystem Interpretation", NCSC-TG-009, Version 1, 16 September 1988

[NCS88c] National Computer Security Center, "A Guide to Understanding Configuration Management in Trusted Systems", NCSC-TG-006, Version 1, 28 March 1988

[NCS88d] National Computer Security Center, "Glossary of Computer Security Terms", NCSC-TG-004-88, 1988

[NCS90] National Computer Security Center, "Trusted Network Interpretation Environment Guideline", NCSC-TG-011, Version 1, 1 August 1990

[NCS91] National Computer Security Center, Trusted Database Management Criteria, 1991

[NIS89] National Institute of Standards and Technology, "Computer Viruses and Related Threats: A Management Guide", NIST Special Publication 500-166, Aug. 1989

[NIS91] National Institute of Standards and Technology, "Reference Model for Frameworks of Software Engineering Environments", NIST Special Publication 500-201, Dec. 91

[RAM91] Rammohan, V., "An Overview of Informix-Online/Secure", Proceedings of the 14th National Computer Conference, Oct. 1991

[RAD89] Rome Air Development Center, "Secure Distributed Data Views", Volumes 1 through V, RADC-TR-89-313, Dec. 1989

[ROM91] U.S. Air Force Rome Laboratory, "System Specification for the CATALYST System", No. Revision 02.00: 1991/05/29 00:00:00, August 1991

[SDI90] Strategic Defense Initiative, "Trusted Software Development Methodology", Volumes 1 and 2, General Electric Aerospace Co., Reports A075-101 and A075-102, Oct. 4, 1990

[SEI91] Software Engineering Institute, "SEI Process Maturity Questionnaire", Report No. SEIC PIR 91123, May 3, 1991

[SII91] Siil, K.A., "Experiences in Multi-Level Security on Distributed Architectures", Proceedings of the 14th National Computer Security Conference, Oct. 1991

[WEI91] Weiss, J., "A System Security Engineering Process", Proceedings of the 14th National Computer Security Conference, Oct. 4, 1991

[WOO87] Woodward, J.P.L., Security Requirements for System High and Compartmented Mode Workstations", MITRE MTR 9992 Revision 1, DIA Document No. DDS-2600-5502-87

VIII. Acronyms

AA	Application Area
ACE	Access Control Encryption
ACM	Access Control Module
ALS	Ada Language System
APSE	Ada Programming Support Environment
AS	Application Specific
ASF/A	Application Specific Subfunction/Activities
BSO	Basic Security Option
CAD	Computer-Aided Design
CAIS	Common APSE Interface Set
CALS	Computer Automated Logistics Support System
CASE	Computer-Aided Software Engineering/Computer-Automated System Engineering
CCB	Configuration Control Board
CIM	Corporate Information Management/Computer-Integrated Manufacturing
CIPSO	Commercial Internet Protocol Security Option
CMM	Capability Maturity Model
CMP	Configuration Management Plan
CMW	Compartmented Mode Workstation
CRAMP	Catalyst Ratings Maintenance Plan
CSL	Computer Systems Laboratory
CSPPM	Catalyst Security Policies & Procedures Manual
DOD	Department of Defense
EIS	Engineering Information System
ESO	Extended Security Option
IDO	Information Domains of
JIAWG	Joint Integrated Avionics Working Group

MCCS	Mission Critical Computer System
MLS	Multi-Level Security
NASA-SSE	NASA Software Support Environment
NASEE	Navy Software Engineering Environment
NCSC	National Computer Security Center
NIST	National Institute for Standards & Technology
OPM	Office of Personnel Management
PCIS	Portable Common Interface Set
PRN	Pseudo Random Number
RAMP	Ratings Maintenance Plan
SCI	Sensitive Compartmented Information
SEAVIEW	Secure Distributed Data Views
SLCSE	Software Life Cycle Support Environment
SOS	Secure Operating System
SSE	Systems Security Engineering
STARS	Software Technology for Adaptable, Reliable Systems
SVA	Security Vulnerability Analysis
SYSEE	Systems Engineering Environment
TCB	Trusted Computer/ing Base
TCM	Trusted Configuration Management
TCMP	Trusted Configuration Management Plan
TCP/IP	Transmission Control Protocol/Internet Protocol
TDB	Trusted Data Base

MISSION

OF

ROME LABORATORY

Rome Laboratory plans and executes an interdisciplinary program in research, development, test, and technology transition in support of Air Force Command, Control, Communications and Intelligence (C^3I) activities for all Air Force platforms. It also executes selected acquisition programs in several areas of expertise. Technical and engineering support within areas of competence is provided to ESD Program Offices (POs) and other ESD elements to perform effective acquisition of C^3I systems. In addition, Rome Laboratory's technology supports other AFSC Product Divisions, the Air Force user community, and other DOD and non-DOD agencies. Rome Laboratory maintains technical competence and research programs in areas including, but not limited to, communications, command and control, battle management, intelligence information processing, computational sciences and software producibility, wide area surveillance/sensors, signal processing, solid state sciences, photonics, electromagnetic technology, superconductivity, and electronic reliability/maintainability and testability.